

STATE OF TEXAS §
 §
COUNTY OF FORT BEND §

**2024 AGREEMENT FOR
EMPLOYEE HEALTH AND WELLNESS CLINICAL SERVICES
PURSUANT TO RFP 25-002**

THIS AGREEMENT is made and entered into by and between Fort Bend County, (hereinafter "County"), a body corporate and politic under the laws of the State of Texas, and Concentra Health Services, Inc., a Nevada Corporation, for the benefit of and on behalf of its subsidiaries, affiliates, and managed professional associations and corporation (hereinafter "Contractor"), a company authorized to conduct business in the State of Texas (collectively referred to as the "Parties").

WITNESSETH

WHEREAS, County desires that Contractor provide Employee Health and Wellness Clinic Services pursuant to and accordance with the requirements of RFP 25-002; and

WHEREAS, Contractor submitted a proposal in response to RFP 25-002 and Contractor represents that it is qualified and desires to perform such Services.

NOW, THEREFORE, in consideration of the mutual covenants and conditions set forth below, the parties agree as follows:

AGREEMENT

Section One. Services

- A. In accordance with the specifications of RFP #25-002, Contractor shall render on-site medical and wellness services to participating county employees and spouses, retirees and dependents (hereinafter "Clinic patients") as described in Exhibit A in accordance with the advertised specifications of RFP, attached as Exhibit C, and the program fees described in Exhibit B to this Agreement. Contractor shall meet or exceed Exhibits A, B, and C, unless requirements are modified by the written agreement of the Parties (hereinafter "Services").

- B. The Parties agree that the Primary Care services to be provided shall include, but are not limited to: health promotion, disease prevention, health maintenance, counseling, patient education, diagnosis and treatment of acute and chronic illnesses which may involve collaborating with other health professionals, and utilizing consultation or referral as appropriate.

- C. Contractor shall design its services to accommodate a minimum of 20 patient appointments each day the clinic is open.
- D. Contractor shall not bill or otherwise solicit payment from Clinic patients, County or from County's group health plan for Services, other than as provided for in the Compensation and Payment Section of this Agreement.
- E. Contractor shall communicate all requests for direction, factual or statistical information relating to Services to the Fort Bend County Risk Management Director. However, the Fort Bend County Risk Management Director shall not serve as the agent of Fort Bend County or the Commissioners Court for any purpose other than conveying factual or statistical information. Contractor may rely on all factual or statistical information supplied by the Fort Bend County Risk Management Director in response to these requests.

Section Two. Compensation and Payment

- A. County shall pay Contractor fees set forth in Exhibit B (the "Fees"). On the earlier of (i) the beginning of each twelve (12) month period after the Effective Date of this Agreement; or (ii) on the anniversary of the commencement date of the existing Agreement between the parties (if applicable), all the Fees provided on Exhibit B (excluding the pass-through items) shall automatically increase three percent (3%). Contractor shall invoice County monthly and County shall remit payment to Contractor as provided in Exhibit B upon receipt of invoice. County agrees to pay any sales, use, excise or similar taxes applicable to the Services provided for hereunder.
- B. Payment shall be made by County within thirty (30) days of receipt of invoice. Contractor may submit invoice(s) electronically in a form acceptable to the County Risk Management Department. Upon execution of this Agreement by both Parties, the County will notify Contractor in writing of the procedure in which Contractor may submit invoice(s) electronically to County. Failure to pay an undisputed portion of invoice when due shall constitute a material breach of this Agreement and Contractor reserves the right to terminate this Agreement pursuant to the remedies set forth in Section 7 (Termination) if the invoice has not been resolved in thirty (30) days of the invoice due date. Contractor reserves the right to refrain from providing Services to County if undisputed charges have not been resolved and paid to Contractor. In the event that Contractor continues to provide Services during a period of time when County is in breach, such continuance of Services will not operate as a waiver of Contractor's right and ability to utilize the remedies available to Contractor under applicable laws.
- C. Any change to this Agreement may only be made by amendment executed by both parties. The written amendment shall include any increase to Fees associated with any requested change to this Agreement.

- D. Mutually approved travel and mileage expenses incurred in the performance of required services will be reimbursed to Contractor to the extent that those costs that do not exceed Fort Bend County travel reimbursement allowances. A copy of the County's Travel Policy with those reimbursement limits is attached and incorporated as Exhibit E to this Agreement. Contractor will not be reimbursed for costs in excess of those listed in Exhibit E.

Section Three. Personnel

- A. Contractor represents that it presently has, or is able to obtain, adequate qualified personnel in its employment for the timely performance of the Services required under this Agreement and that Contractor shall furnish and maintain, at its own expense, adequate and sufficient personnel, in the opinion of County, to perform the Services when and as required and without delays.
- B. All employees of Contractor shall have such knowledge and experience as will enable them to perform the duties assigned to them. Any employee of Contractor who, in the opinion of County, is incompetent or by their conduct becomes detrimental to the project shall, upon request of County, immediately be removed from association with the project.
- C. All persons (whether Contractor's employees or Contractor's contractors) providing services under this Agreement shall submit to a background investigation conducted by the County's Human Resources Department. County may accept a criminal background investigation consisting of a minimum of five (5) years state and federal inquiry conducted by Contractor if conducted within the ninety (90) days of hire by Contractor.
- D. At all times during the Agreement, Contractor shall ensure that Contractor's personnel maintain in good standing all professional license(s) and accreditation(s) applicable to Services. Contractor shall perform all acts necessary to ensure that Contractor's personnel maintain and improve their professional competence and training. Contractor shall notify County within two (2) business days if any adverse action related to personnel professional license(s) or accreditation(s) occurs.

Section Four. Use of Clinic Space by Contractor

- A. Services shall be provided by Contractor at a County owned or leased building, hereinafter referred to as "the Clinic," as determined by County, which Contractor may use only for the purpose of providing health and wellness clinic operation services for County. The Clinic is located at 301 Jackson Street, Richmond Texas. Except as may be stated in writing provided to County, Contractor has inspected the Clinic and found it acceptable in "as is" condition for the performance of the Services.
- B. Any and all improvements of the Clinic, including any changes, modifications or

additions, requested by Contractor shall be reviewed and approved in advance by County's Facilities Management & Planning Department Director and County's Risk Manager, and shall, if approved, be constructed by County and funded by County unless otherwise mutually agreed by the Parties. Any and all improvements to the Clinic shall become part of the Clinic and shall remain subject to this Agreement and shall be surrendered by Contractor upon termination of this Agreement. Personal property, furniture, and equipment removable without damage to the Clinic structure and paid for by Contractor shall remain the property of Contractor at all times.

- C. Contractor shall have the right to erect graphics or signs within or upon the Clinic, provided that: (1) Contractor shall bear the cost of all graphics or signs placed within the Clinic; and (2) all graphics and signs shall be approved in advance by County's Facilities Management & Planning Department Director and County's Risk Manager.
- D. County shall not be responsible for any loss or damage to any equipment or supplies of Contractor, its agents, employees or subcontractors, unless such loss or damage is proven to have been caused by the negligence of County. Contractor shall immediately report any and all lost items to County.
- E. Contractor shall be responsible for the lawful disposal of hazardous medical waste generated within the Clinic and those other items that the parties mutually agree to in writing after the commencement date of this Agreement. Contractor shall keep the Clinic in a clean, safe and attractive condition. County shall be responsible for utilities and facility maintenance of the Clinic to include the foundation, roof, exterior walls, main plumbing, central heating and cooling, utilities and custodial services.
- F. It is the responsibility of Contractor to promptly notify County's Facilities Department when maintenance/repair service is required including service for medical equipment. Contractor shall utilize the County Work Order system for all repairs and replacements which must be approved by County's Facilities Department prior to maintenance or repair service commencing.

Section Five. Limit of Appropriation

- A. Contractor understands and agrees that the total Maximum Compensation for the performance of the Services within the Scope of Services described in Section One of this Agreement is one million six hundred nineteen thousand, six hundred and seventy-eight (\$1,619,678) for year 1, and one million six hundred twenty one thousand, eight hundred and five (\$1,621,805) for year 2, plus any additional amounts of funds from time to time that may be certified as available, as of the date so certified, by the County Auditor pursuant to Sections 111.061 through 111.073 of the Local Government Code, as amended, for the purpose of satisfying County's obligations under the terms and provisions of this Agreement; and that when and if all the funds so certified are expended for the purpose of satisfying County's obligations under the terms and provisions of this Agreement, the sole and exclusive remedy of Contractor is to terminate this

Agreement. In no event shall the amount paid by County under this Agreement exceed the total Maximum Compensation and any additional amounts that may be certified as available below by the County Auditor. without a County approved change order.

- B. Contractor further understands and agrees, such understanding and agreement being of the absolute essence of this Agreement, that County shall have available the total maximum sum of one million six hundred nineteen thousand, six hundred and seventy-eight (\$1,619,678) for year 1, and one million six hundred twenty one thousand, eight hundred and five (\$1,621,805) for year 2, and any additional amounts that may be certified as available below by the County Auditor, specifically allocated to fully discharge any and all liabilities County may incur under this Agreement.
- C. Contractor further understands and agrees, said understanding and agreement also being of the absolute essence of this Agreement, that the total Maximum Compensation that Contractor may become entitled to and the total maximum sum that County may become liable to pay to Contractor under this Agreement shall not under any conditions, circumstances, or interpretations thereof exceed one million six hundred nineteen thousand, six hundred and seventy-eight (\$1,619,678) for year 1, and one million six hundred twenty one thousand, eight hundred and five (\$1,621,805) for year 2, and any additional amounts that may be certified as available below by the County Auditor.
- D. Contractor further understands and agrees that this Limit of Appropriations is not a guarantee that Contractor will receive the entire amount of one million six hundred nineteen thousand, six hundred and seventy-eight (\$1,619,678) for year 1, and one million six hundred twenty one thousand, eight hundred and five (\$1,621,805) for year 2, but a statement that all fees and additional costs for this Agreement, when combined, shall not exceed said amount.

Section Six. Term

The term of this Agreement shall be for a period of twenty four (24) months, commencing on January 2, 2025, and ending at the close of business on January 1, 2027, with three (3) additional one-year renewal options on the same terms and conditions at County's sole discretion. Either party shall have the right to terminate this Agreement as provided herein.

Section Seven. Termination

- A. Termination for Non-Appropriation: County shall have the right to terminate this Agreement in the event of non-appropriation of funds by the County's governing body. County shall provide Contractor with ninety (90) days

advanced written notice of such non- appropriation termination. County shall compensate Contractor, in accordance with the fee schedule as provided in Exhibit B, for Services provided proper to the date of termination specified in the notice. Contractor shall not be entitled to lost or anticipated profits should County choose to exercise its option to terminate for non-appropriation of funds.

B. Termination for Convenience: Either Party may terminate this Agreement at any time upon 150 days written notice.

C. Termination for Default

1. This Agreement may be terminated in whole or part for cause in the following circumstances:

a. If Contractor fails to perform services within the time specified in the Scope of Services or any extension thereof granted by the County in

b. If either party materially breaches any of the covenants or terms and conditions set forth in this Agreement or fails to perform any of the other provisions of this Agreement or so fails to make progress as to endanger performance of this Agreement in accordance with its terms, and in any of these circumstances does not cure such breach or failure to the other Party's reasonable satisfaction within a period of thirty (30) calendar days after receipt of notice specifying such breach or failure.

2. If, after termination, it is determined for any reason whatsoever that a party was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for convenience in accordance with Section 7A above.

D. Upon termination of this Agreement, County shall compensate Contractor in accordance with the Compensation and Payment Section above, for those services which were provided under this Agreement prior to its termination and which have not been previously invoiced to County. Contractor's final invoice for said services will be presented to and paid by County in the same manner set forth in the Compensation and Payment Section above.

E. If County terminates this Agreement as provided in this Section, no fees of any type, other than fees due and payable at the Termination Date, shall thereafter be paid to Contractor.

Section Eight. Modifications and Waivers

- A. The parties may not amend or waive this Agreement, except by a written agreement executed by both parties.
- B. No failure or delay in exercising any right or remedy or requiring the satisfaction of any condition under this Agreement, and no course of dealing between the parties, operates as a waiver or estoppel of any right, remedy, or condition.
- C. The rights and remedies of the parties set forth in this Agreement are not exclusive of, but are cumulative to, any rights or remedies now or subsequently existing at law, in equity, or by statute.

Section Nine. Inspection of Books and Records

Contractor will permit County, or any duly authorized agent of County, to inspect and examine the books and non-patient identified records of Contractor for the purpose of verifying the amount of work performed under the Scope of Services. County may review any and all of the Services performed by Contractor pursuant to this Agreement, along with the use and occupancy of the Clinic authorized under this Agreement. County's right to inspect survives the termination of this Agreement for a period of four years.

Section Ten. Medical Records

- A. Contractor shall maintain complete and accurate electronic medical records (hereinafter "EMR") for each Clinic patient. For purposes of this Agreement, an EMR is a real-time transaction processing database of medical information. Records will be kept in a professional and legally compliant manner consistent with the accepted practices of the professional medical community.
- B. All medical records maintained by Contractor in connection with this Agreement shall be property of each individual patient and Contractor shall be the custodian of the records and data during the term of this Agreement. Contractor shall comply with all federal and state medical record requirements including but not limited to the Health Insurance Portability and Accountability Act. Contractor will at all times comply and require that any subcontractor comply with all applicable provisions of such laws, regulations and policies. The confidentiality of personal health information, as defined by HIPAA, that may be shared between Contractor and County's Third Party Administrator is covered and governed by a Business Records Associate Agreement.
- C. County understands and agrees that all of the medical records and other protected health information maintained by Contractor will be held in the strictest confidence. County is not entitled to access to the patient identified medical records or protected health information of Clinic patents without the appropriate written authorization from the patient unless medical records are a result of occupational medical services provided (i.e. Worker's Compensation or Pre-Employment Physicals) or as otherwise

permitted by law.

- D. The retention of all medical records shall be in compliance with applicable State and Federal laws and it is the responsibility of Contractor to ensure compliance. Contractor shall develop and implement policies, standards and procedure to protect the confidentiality and security of the medical records and ensure that all employees are trained to adhere to security requirements similar to Exhibit F.
- E. Upon termination of this Agreement, Contractor shall provide notice to all patients and facilitate the transfer of patient medical records to a provider as designated by each patient. Upon request of any patient at any time and payment of a reasonable copy fee, Contractor shall provide patient a copy of patient's medical record. At no time shall the County be the custodian of any medical records and/or data of any patient.
- F. Upon the termination of this Agreement for any reason, County shall negotiate the execution of a custodial agreement with Contractor and any new third-party medical provider ("**New Medical Provider**"), as applicable, to ensure all parties' compliance with applicable laws. Contractor shall provide County with such custodial agreement for its review. Contractor agrees and understands that execution by the County of any subsequent custodial agreement may require approval by the County's Commissioners Court. County shall be solely responsible for any expense related to the transfer of medical records, including, but not limited to those arising from any retention of records required by law (including OSHA), any photocopies requested, any records/data requested to be provided in an electronic format and/or transferred to the County or New Medical Provider(s), and such actual fees charged by electronic medical records vendors. The records shall be inclusive of all historical medical records related to the patient population of the Onsite Center(s).

County shall be invoiced for any production/conversion as a separate line item as a standard Service under this Agreement, which must be paid in full prior to the release of the final set of data requested by County or New Medical Provider(s). If historical medical records were provided to Contractor by County or any third-party, such historical records shall be provided to County or New Medical Provider(s) in the same manner and condition as provided to Contractor. Upon payment by County, the parties will make best efforts to deliver and/or transfer such records within two (2) weeks, or a mutually agreed upon date.

If Contractor is replacing an existing third-party medical provided (a "**Prior Medical Provider**") as part of a transition of service at the Onsite Center, Contractor shall become the medical record custodian as of the open for business date of the Onsite Center and all parties should execute a custodial agreement thirty (30) days prior to the Onsite Center anticipated open for business date to ensure all parties' compliance with applicable laws. County shall provide Contractor written notice of the intended format and delivery of all records created to Contractor sixty (60) days prior to the anticipated open for business date. Such delivery shall include any medical records, required data, software applications previously used, and required data conversions proposed. It is understood and agreed that the transfer of medical records of any patients of a Prior Medical Provider to Contractor may require a Prior Medical Provider to first notify its patients and facilitate the transfer of patient medical records to a provider as designated

by each patient. Any fees associated with such transfer of the above materials from the Prior Medical Provider shall be at the County's sole expense.

Section Eleven. Insurance

A. Prior to commencement of the Services, Contractor shall furnish County with properly executed certificates of insurance which shall evidence all insurance required and provide that such insurance shall not be canceled, except on 30 days' prior written notice to County. Contractor shall provide certified copies of insurance endorsements and/or policies if requested by County. Contractor shall maintain such insurance coverage from the time Services commence until Services are completed and provide replacement certificates, policies and/or endorsements for any such insurance expiring prior to completion of Services. Contractor shall obtain such insurance written on an Occurrence form from such companies having Bests rating of A/VII or better, licensed or approved to transact business in the State of Texas, and shall obtain such insurance of the following types and minimum limits:

1. Workers' Compensation insurance in accordance with the laws of the State of Texas. Substitutes to genuine Workers' Compensation Insurance will not be allowed. Employers' Liability insurance with limits of not less than \$1,000,000 per injury by accident, \$1,000,000 per injury by disease, and \$1,000,000 per bodily injury by disease.
2. Commercial general liability insurance with a limit of not less than \$1,000,000 each occurrence and \$2,000,000 in the annual aggregate. Policy shall cover liability for bodily injury, personal injury, and property damage and products/completed operations arising out of the business operations of the policyholder.
3. Professional Medical Malpractice Liability Insurance: Professional Medical Malpractice Liability Insurance shall be maintained with limits of no less than \$1,000,000 per occurrence and \$3,000,000 in aggregate.

B. County and the members of Commissioners Court shall be named as additional insured to all required coverage except for Workers' Compensation and Professional Medical Malpractice Liability.

C. All Liability policies written on behalf of Contractor shall contain a waiver of subrogation in favor of County and members of Commissioners Court.

D. If required coverage is written on a claims-made basis, Contractor warrants that any retroactive date applicable to coverage under the policy precedes the effective date of the Contract and that continuous coverage will be maintained or an extended discovery period will be exercised for a period of 2 years beginning from the time the work under this Contract is completed.

E. Contractor shall not commence any portion of the work under this Contract until it

has obtained the insurance required herein and certificates of such insurance have been filed with and approved by Fort Bend County.

- F. No cancellation of or changes to the certificates, or the policies, may be made without thirty (30) days prior, written notification to Fort Bend County.
- G. Approval of the insurance by Fort Bend County shall not relieve or decrease the liability of the Contractor.

Section Twelve. Indemnity

A. CONTRACTOR AGREES TO HOLD HARMLESS COUNTY, ITS AGENTS AND EMPLOYEES FROM ANY AND ALL CLAIMS, ACTIONS, LAWSUITS, DAMAGES, JUDGMENTS OR LIABILITIES OF ANY KIND WHATSOEVER ARISING OUT OF THE NEGLIGENT OPERATION AND MAINTENANCE OF THE AFORESAID PROGRAM OF HEALTH CARE SERVICES AS CONDUCTED BY CONTRACTOR, ITS EMPLOYEES OR AGENTS, IT BEING THE EXPRESS UNDERSTANDING OF THE PARTIES HERETO THAT CONTRACTOR SHALL PROVIDE THE ACTUAL HEALTH CARE SERVICES, AND HAVE COMPLETE RESPONSIBILITY FOR SUCH HEALTH CARE SERVICES PROVIDED BY ITS EMPLOYEES AND AGENTS AND ANY LAWSUIT ARISING SOLELY OUT OF SUCH DELIVERY OF HEALTHCARE.

- B. Contractor shall timely report all such matters to County and shall, upon the receipt of any such claim, demand, suit, action, proceeding, lien or judgment, not later than the fifteenth day of each month; provide County with a written report on each such matter, setting forth the status of each matter, the schedule or planned proceedings with respect to each matter and the cooperation or assistance, if any, of County required by Contractor in the defense of each matter.
- C. Contractor's duty to defend, indemnify and hold County harmless shall be absolute. It shall not abate or end by reason of the expiration or termination of any contract unless otherwise agreed by County in writing. The provisions of this section shall survive the termination of the contract and shall remain in full force and effect with respect to all such matters no matter when they arise.
- D. In the event of any dispute between the Parties as to whether a claim, demand, suit, action, proceeding, lien or judgment appears to have been caused by or appears to have arisen out of or in connection with acts or omissions of Contractor, Contractor shall never-the-less fully defend such claim, demand, suit, action, proceeding, lien or judgment until and unless there is a determination by a court of competent jurisdiction that the acts and omissions of Contractor are not at issue in the matter.
- E. Contractor's indemnification shall cover, and Contractor agrees to indemnify County, in the event County is found to have been negligent for having selected Contractor to perform the work described in this request.
- F. The provision by Contractor of insurance shall not limit the liability of Contractor under this Agreement.

- G. As applicable, Contractor shall cause all trade contractors and any other contractor who may have a contract to perform construction or installation work in the area where work will be performed under this Agreement, to agree to indemnify County and to hold it harmless from all claims for bodily injury and property damage that may arise from Contractor's operations. Such provisions shall be in form satisfactory to County.
- H. County shall be exempt from, and in no way liable for, any sums of money which may represent a deductible in any insurance policy. The payment of deductibles shall be the sole responsibility of Contractor and/or trade contractor providing such insurance.

Section Thirteen. Confidential and Proprietary Information

- A. Contractor acknowledges that it and its employees or agents may, in the course of performing their responsibilities under this Agreement, be exposed to or acquire information that is confidential to County. Any and all information of any form obtained by Contractor or its employees or agents from County in the performance of this Agreement shall be deemed to be confidential information of County ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated with respect to confidentiality in the same manner as the Confidential Information. Confidential Information shall be deemed not to include information that (a) is or becomes (other than by disclosure by Contractor) publicly known or is contained in a publicly available document; (b) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Agreement; or (c) is independently developed by employees or agents of Contractor who can be shown to have had no access to the Confidential Information.
- B. Contractor agrees to hold Confidential Information in strict confidence, using at least the same degree of care that Contractor uses in maintaining the confidentiality of its own confidential information, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than the provision of Services to County hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use its best efforts to assist County in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limitation of the foregoing, Contractor shall advise County immediately in the event Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Agreement and Contractor will at its expense cooperate with County in seeking injunctive or other equitable relief in the name of County or Contractor against any such person. Contractor agrees that, except as directed by County, Contractor will not at any time during or after the term of this Agreement disclose, directly or indirectly, any Confidential Information to any person, and that upon termination of this Agreement or at County's request, Contractor will promptly

turn over to County all documents, papers, and other matter in Contractor's possession which embody Confidential Information.

- C. Contractor acknowledges that a breach of this Section, including disclosure of any Confidential Information, or disclosure of other information that, at law or in equity, ought to remain confidential, will give rise to irreparable injury to County that is inadequately compensable in damages. Accordingly, County may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interest of County and are reasonable in scope and content.
- D. Contractor in providing all services hereunder agrees to abide by the provisions of any applicable Federal or State Data Privacy Act.
- E. Contractor expressly acknowledges that County is subject to the Texas Public Information Act, TEX. GOV'T CODE ANN. §§ 552.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, County will make any information related to the Agreement, or otherwise, available to third parties in accordance with the Texas Public Information Act. Any proprietary or confidential information marked as such provided to County by Consultant shall not be disclosed to any third party, except as directed by the Texas Attorney General in response to a request for such under the Texas Public Information Act, which provides for notice to the owner of such marked information and the opportunity for the owner of such information to notify the Attorney General of the reasons why such information should not be disclosed. The terms and conditions of the Agreement are not proprietary or confidential information.
- F. Contractor expressly acknowledges that County is subject to the Texas Open Meetings Act, TEX. GOV'T CODE ANN. §§ 551.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, County will comply with the provisions of the Texas Open Meetings Act in relation to the Agreement.

Section Fourteen. Independent Contractor

The relationship of the parties under this Agreement is that Contractor is an independent contractor. To the extent Contractor performs Services under this Agreement, it shall do so solely in the capacity of an independent contractor in its relationship with County. Contractor shall exercise independent judgment in making all medical decisions with respect to its patients and in managing and operating the Clinic pursuant to this Agreement, and is solely responsible for making medical decisions, scheduling, prioritizing, staffing clinic operations, and determining how Clinic operations are to be performed. No term or provision of this Agreement or act of Contractor during the term of this Agreement shall be construed as making Contractor the agent, servant or employee of County, or making Contractor or any of its employees eligible for the fringe benefits,

such as retirement, insurance and worker's compensation, which County provides to its employees. No term or provision of this Agreement or act of Contractor in performing under the terms of this Agreement shall be construed as creating a partnership, joint venture, or joint enterprise, or making Contractor the agent, servant, employee, partner or joint venturer of County.

Section Fifteen. Notices

- A. Each party giving any notice or making any request, demand, or other communication (each, a "Notice") pursuant to this Agreement shall do so in writing and shall use one of the following methods of delivery, each of which, for purposes of this Agreement, is a writing: personal delivery, registered or certified mail (in each case, return receipt requested and postage prepaid), or nationally recognized overnight courier (with all fees prepaid).
- B. Each party giving a Notice shall address the Notice to the receiving party at the address listed below or to another address designated by a party in a Notice pursuant to this Section:

County: Fort Bend County
Attn: County Judge
401 Jackson Street
Richmond, Texas 77469

With a copy to: Fort Bend County Risk Management
Attn: Director
301 Jackson, Suite 224
Richmond, Texas 77469

Contractor: Concentra Health Services, Inc.
5080 Spectrum Drive, Suite 1200W
Addison, Texas 75001
Attn: Legal – Contracting (Onsites)

With a copy to: Concentra Health Services, Inc.
5080 Spectrum Drive, Suite 1200W
Addison, Texas 75001
Attn: Michael Rhine – EVP & Chief Operating Officer-
Onsite Health and Telemed

- C. Notice is effective only if the party giving or making the Notice has complied with subsections 15 (A) and 15 (B) and if the addressee has received the Notice. A Notice is deemed received as follows:
 - 1. If the Notice is delivered in person, or sent by registered or certified mail or a nationally recognized overnight courier, upon receipt as

indicated by the date on the signed receipt.

2. If the addressee rejects or otherwise refuses to accept the Notice, or if the Notice cannot be delivered because of a change in address for which no Notice was given, then upon the rejection, refusal, or inability to deliver.

Section Sixteen. Compliance with Laws

Contractor shall comply with all federal, state, and local laws, statutes, ordinances, rules and regulations, and the orders and decrees of any courts or administrative bodies or tribunal in any matter affecting the performance of this Agreement, including, without limitation, Worker's Compensation laws, minimum and maximum salary and wage statutes and regulations, licensing laws and regulations. When required by County, Contractor shall furnish County with certification of compliance with said laws, statutes, ordinances, rules, regulations, orders, and decrees above specified. Nothing in this Agreement will be construed to waive the requirements of any record retention laws applicable to County.

Section Seventeen. Performance Warranty

- A. Contractor warrants to County that Contractor has the skill and knowledge ordinarily possessed by well-informed members of its trade or profession practicing in the greater Houston metropolitan area and Contractor will apply that skill and knowledge with care and diligence to ensure that the Services provided hereunder will be performed and delivered in accordance with the highest professional standards, and in accordance with the requirements and specifications of this Agreement.
- B. Contractor shall continue meeting mutually agreed upon Performance Indicators/Objectives described in Exhibit D. and agrees to place up to twenty percent (20%) of its administration fee at risk as outlined in Exhibit D. Contractor will prepare a monthly report stating its performance by Performance Indicator. The report will be provided to Fort Bend County Risk Manager with a copy to Fort Bend County Purchasing Agent within 15 days after the end of the month covered in the report. While performance will be monitored monthly, liquidated damages, if any, will be the percentage of Contractor's administration fee based on the annual performance results upon a final determination that a performance standard has not been met. Any payment from Contractor will be paid to County, if due, annually by Contractor, or offset at County's option, from payments due in the following month's invoice after liquidated damages have been determined.

Section Eighteen. Assignment and Delegation

- A. Neither party may assign any of its rights under this Agreement, except with the prior written consent of the other party. That party shall not unreasonably withhold its consent. All assignments of rights are prohibited under this

subsection, whether they are voluntarily or involuntarily, by merger, consolidation, dissolution, operation of law, or any other manner.

- B. Neither party may delegate any performance under this Agreement.
- C. Any purported assignment of rights or delegation of performance in violation of this Section is void.

Section Nineteen. Applicable Law

The laws of the State of Texas govern all disputes arising out of or relating to this Agreement. The parties hereto acknowledge that venue is proper in Fort Bend County, Texas, for all legal actions or proceedings arising out of or relating to this Agreement and waive the right to sue or be sued elsewhere. Nothing in the Agreement shall be construed to waive the County's sovereign immunity. County does not agree to submit disputes arising out of the Agreement to binding arbitration. County does not agree to pay any and/or all attorney fees incurred by Contractor in any way associated with the Agreement.

Section Twenty. Successors and Assigns

County and Contractor bind themselves and their successors, executors, administrators and assigns to the other party of this Agreement and to the successors, executors, administrators and assigns of the other party, in respect to all covenants of this Agreement.

Section Twenty-One. Third Party Beneficiaries

This Agreement does not confer any enforceable rights or remedies upon any person other than the parties.

Section Twenty-Two. Severability

If any provision of this Agreement is determined to be invalid, illegal, or unenforceable, the remaining provisions remain in full force, if the essential terms and conditions of this Agreement for each party remain valid, binding, and enforceable.

Section Twenty-Three. Publicity

Contact with citizens of Fort Bend County, media outlets, or governmental agencies shall be the sole responsibility of County. Under no circumstances whatsoever, shall Contractor release any material or information developed or received in the performance of the Services hereunder without the express written permission of County, except where required to do so by law.

Section Twenty-Four. Captions

The section captions used in this Agreement are for convenience of reference only and do not affect the interpretation or construction of this Agreement.

Section Twenty-Five. Certain State Law Requirements for Contracts

The contents of this Section are required by Texas law and are included by County regardless of content For purposes of Sections 2252.152, 2271.002, and 2274.002, Texas Government Code, as amended, Contractor hereby verifies that Contractor and any parent company, wholly owned subsidiary, majority-owned subsidiary, and affiliate:

- A. Unless affirmatively declared by the United States government to be excluded from its federal sanctions regime relating to Sudan or Iran or any federal sanctions regime relating to a foreign terrorist organization, is not identified on a list prepared and maintained by the Texas Comptroller of Public Accounts under Section 806.051, 807.051, or 2252.153 of the Texas Government Code.
- B. If employing ten (10) or more full-time employees and this Agreement has a value of \$100,000.00 or more, Contractor does not boycott Israel and is authorized to agree in such contracts not to boycott Israel during the term of such contracts. "Boycott Israel" has the meaning provided in § 808.001 of the Texas Government Code.
- C. If employing ten (10) or more full-time employees and this Agreement has a value of \$100,000.00 or more, Contractor does not boycott energy companies and is authorized to agree in such contracts not to boycott energy companies during the term of such contracts. "Boycott energy company" has the meaning provided in § 809.001 of the Texas Government Code.
- D. If employing ten (10) or more full-time employees and this Agreement has a value of \$100,000.00 or more, Contractor does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and is authorized to agree in such contracts not to discriminate against a firearm entity or firearm trade association during the term of such contracts. "Discriminate against a firearm entity or firearm trade association" has the meaning provided in § 2274.001(3) of the Texas Government Code. "Firearm entity" and "firearm trade association" have the meanings provided in § 2274.001(6) and (7) of the Texas Government Code.

Section Twenty-Six. Human Trafficking

BY ACCEPTANCE OF CONTRACT, CONTRACTOR ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.

Section Twenty-Seven. Entire Agreement

This Agreement contains the entire Agreement among the parties and supersedes all other negotiations and agreements, whether written or oral. Attached hereto is Exhibit A: Scope of Work; Exhibit B: Program Fees; Exhibit C: *RFP #25-002 Employee Clinical Services*;

Exhibit D: Performance Indicators/Objectives; Exhibit E: *County Travel Policy*; and Exhibit G: Information Systems and Technology all of which are incorporated by reference as if set forth herein verbatim for all purposes.

Section Twenty-Eight. Modifications and Conflict

In the event there is a conflict among the documents that make up this Agreement, the following shall have priority with regard to the conflict: (1) this document titled 2024 AGREEMENT FOR EMPLOYEE HEALTH AND WELLNESS CLINICAL SERVICES, (2) County's RFP 25-002 (Exhibit C), (3) County Travel Policy (Exhibit E), (4) Scope of Work (Exhibit A), (5) Program Fees (Exhibit B), (6) Performance Indicators/Objectives (Exhibit D), and (7) Information Systems and Technology (Exhibit G), and (8) Security Requirements (Exhibit F).

Section Twenty-Nine. Information Systems

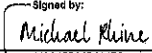
County shall comply with Contractor's technology components and Security requirements required to perform the Services as provided in Exhibit G. Contractor will provide its standard software/hardware and systems support required to deliver the Services. Contractor may, at its discretion, upgrade and make changes to the software platform and hardware utilized at the Onsite Center. Fees associated with such upgrades and changes shall be the responsibility of Contractor unless otherwise mutually agreed to by the Parties.

Section Thirty. Further Assurances. Each party further agrees that it shall take any and all necessary steps and sign and execute any and all necessary documents or agreements required to implement the terms of the Agreement of the Parties contained in this contract, and each party agrees to refrain from taking any action, either expressly or impliedly, which would have the effect to prohibiting or hindering the performance of the other party to this Agreement.

(Execution Page Follows)

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, the parties hereto have signed or have caused their respective names to be signed to multiple counterparts to be effective on the _____ day of _____, 2024.

| | |
|--|-------------------------|
| Concentra Health Services, Inc. | Fort Bend County |
| Signature: _____ | Signature: _____ |
| <small>Signed by:</small>  | |
| Name: Michael Rhine | Name: _____ |
| Title: EVP & Chief Operating Officer, Onsites | Title: _____ |
| Date: 12/9/2024 | Date: _____ |

ATTEST:

Laura Richard, County Clerk

REVIEWED:



Risk Management Department

Attachments:

- Exhibit A – Scope of Work
- Exhibit B – Program Fees
- Exhibit C – RFP 25-002
- Exhibit D – Performance Indicators/Objectives
- Exhibit E – County Travel Policy
- Exhibit F – Security Requirements
- Exhibit G - Information Systems and Technology

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of **\$ 3,241,483.00** are available to pay the obligation of Fort Bend County within the foregoing Agreement for services provided by Contractor for the below time period:

January 2, 2025 – January 1, 2027
Service Period

Robert Ed Sturdivant, County Auditor

Date Certified

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of \$_____ are available to pay the obligation of Fort Bend County within the foregoing Agreement for services provided by Contractor for the below time period:

Service Period

Robert Ed Sturdivant, County Auditor

Date Certified

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of \$_____ are available to pay the obligation of Fort Bend County within the foregoing Agreement for services provided by Contractor for the below time period:

Service Period

Robert Ed Sturdivant, County Auditor

Date Certified

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of \$_____ are available to pay the obligation of Fort Bend County within the foregoing Agreement for services provided by Contractor for the below time period:

Service Period

Robert Ed Sturdivant, County Auditor

Date Certified

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of \$_____ are available to pay the obligation of Fort Bend County within the foregoing Agreement for services provided by Contractor for the below time period:

Service Period

Robert Ed Sturdivant, County Auditor

Date Certified

(Exhibits on following pages)

(Remainder of Page Intentionally Left Blank)

**EXHIBIT A
SCOPE OF WORK (“SOW”)**

1. Location. Services provided at the following location:

| Onsite Center address | City, State, Zip | Onsite Contact |
|-----------------------|--------------------|--|
| 301 Jackson Street | Richmond, TX 77469 | Wyatt Scott, Director of Risk Management 281.341.4493 Wyatt.scott@fortbendcountytexas.gov |

2. Statement of Work

Please note that services listed are examples and may not reflect the full capabilities of the role; staff will perform clinical services as agreed upon by the client and governed by their licensure/certification and State Practice Act.

| | |
|--|---|
| <input checked="" type="checkbox"/> Occupational Health – Provider-based <ul style="list-style-type: none"> • Work-related injury/illness treatment - provider • Medical Examinations <ul style="list-style-type: none"> ○ Dept. of Transportation exams ○ General Physicals (i.e., preplacement, return to work, fitness for duty) ○ Surveillance – (i.e., OSHA, NFPA) <input checked="" type="checkbox"/> Occupational Health – Medical Support (RN/MA) <ul style="list-style-type: none"> • Work-related injury/illness triage/assessment - RN • Clinical testing <ul style="list-style-type: none"> ○ Audiograms ○ Pulmonary function ○ Respirator fit ○ Vision/Titmus • Drug and alcohol testing/collections • Laboratory collections • Vaccine Administration/Injections • Assessments <ul style="list-style-type: none"> ○ Injury prevention training ○ Ergonomic assessments ○ Functional job analysis/functional testing | <input checked="" type="checkbox"/> Acute Episodic (Urgent) Care <ul style="list-style-type: none"> • Upper respiratory infections • Headache • Sore throat • Non-work-related sprains/strains • Lacerations • Gastrointestinal issues/urinary tract infections • Skin irritation/rash <input checked="" type="checkbox"/> Primary Care <ul style="list-style-type: none"> • Chronic disease management • Preventive care • Lifestyle medicine • Routine gender/age-specific exams and screenings • Laboratory collections • Immunizations • Medication management • Care coordination |
| <input type="checkbox"/> Travel Medicine <ul style="list-style-type: none"> • Vaccination/medication administration in accordance with WHO and CDC recommendations • Physical examination services – country-specific | <input checked="" type="checkbox"/> Pharmacy <ul style="list-style-type: none"> • Depending on state law, provide may prescribe or dispense • Texas does not allow clinician dispensing – onsite clinicians will e-Prescribe |
| <input type="checkbox"/> Emergency Response Services – EMT-P <ul style="list-style-type: none"> • First aid treatment per standing orders • Work-related injury/illness assessment • Emergency patient transport facilitation • Clinical testing (as trained/certified) • Administrative clinic duties | <input checked="" type="checkbox"/> Health Improvement/Wellness Services <ul style="list-style-type: none"> • Biometric screens • Health risk assessments • Health fairs • Health education (monthly) |
| <input type="checkbox"/> Physical Therapy <u>Injury Assessment & Rehabilitation:</u> <ul style="list-style-type: none"> • Electrical modalities • Therapeutic exercise • Flexible taping • Manual therapy/joint manipulation • Dry needling | <input type="checkbox"/> Athletic Trainer <u>Injury Assessment & Rehabilitation:</u> <ul style="list-style-type: none"> • Electrical modalities • Exercise/Massage • Flexible taping • Work conditioning |

| | |
|--|---|
| <ul style="list-style-type: none"> • Work conditioning <p><u>MSD First Aid Services:</u></p> <ul style="list-style-type: none"> • Early reporting MSD assessment/1st Aid <p><input type="checkbox"/> Physical Therapy (cont.)</p> <p><u>Non-Injury Services</u></p> <ul style="list-style-type: none"> • Office & industrial ergonomic assessment • Functional job analyses • Wellness & preventive services • Return to work & fit-for-duty management • Injury prevention training • Preventative musculoskeletal screening • Post-offer, pre-placement functional testing • Preventive stretching and exercise programs | <p><u>MSD First Aid Services:</u></p> <ul style="list-style-type: none"> • Early reporting MSD assessment/1st Aid <p><u>Non-MSD First Aid:</u></p> <ul style="list-style-type: none"> • Non-Musculoskeletal First Aid/Emergency mgmt <p><input type="checkbox"/> Athletic Trainer (cont.)</p> <p><u>Non-Injury Services:</u></p> <ul style="list-style-type: none"> • Office & industrial ergonomic assessment • Functional job analyses • Wellness & preventive services • Return to work & fit-for-duty management • Injury prevention training • Preventative musculoskeletal screening • Post-offer, pre-placement functional testing • Preventive stretching and exercise programs |
| <p><input type="checkbox"/> Ancillary Services</p> <ul style="list-style-type: none"> • Massage therapy • Chiropractic • Acupuncture • Behavioral health services | |

3. Staffing:

Concentra agrees to provide the following staff:

| Clinician Staff | | | |
|--|-----------|----------------|---|
| | FTE Count | Hours Per Week | Backfill/Coverage |
| Physician Oversight (PO) | | Provided | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Center Medical Director (CMD) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Staff Physician(s) (MD/DO) | 1.0 | 40 | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Advanced Practice Clinician (NP/PA) | 1.5 | 60 | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Clinical Support, Therapy, and Operational Staff | | | |
| | FTE Count | Hours Per Week | Backfill/Coverage |
| Registered Nurse (RN) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| RN Case Manager/Care Coordinator | | | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Certified Occupational Health Nurse (COHN) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Licensed Practical/Vocational Nurse (LPN/LVN) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Medical Assistant (MA) | 1.0 | 40 | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Medical Assistant/X-ray/Ultrasound Technician | 2.0 | 80 | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Emergency Medical Technician (EMT-P) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Physical Therapist (PT) | | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Athletic Trainer (AT) | | | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Certified Health Educator/ Dietitian (RD) | .5 | 20 | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Clinic Operations Director (COD) | | | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Health Coach (HC) | | | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

4. Hours of Operation:

| Saturday | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday |
|----------|--------|---------|---------|-----------|----------|---------|
| 8am-4pm | NA | 7am-6pm | 7am-6pm | 7am-6pm | 7am-6pm | 7am-6pm |

*The hours of operation set forth in this Exhibit A are the general hours the Onsite Center will be open. Specific services may be offered at various times within the hours of operation as agreed to by the parties in writing and as adjusted from time to time.

5. Holidays:

New Year's Day Staffed Not Staffed
 Memorial Day Staffed Not Staffed

| | | |
|-----------------------------------|----------------------------------|---|
| Independence Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Labor Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Thanksgiving Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Christmas Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Additional Holidays: | | |
| Birthday of Martin Luther King Jr | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Good Friday | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Juneteenth | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Fort Bend County Fair Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Veterans Day | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Day after Christmas | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |
| Day after Thanksgiving | <input type="checkbox"/> Staffed | <input checked="" type="checkbox"/> Not Staffed |

6. Eligible Participants (Check all that Apply):

- Employees
- Spouses
- Dependents - children
 - Age 5 and older
- Retirees

7. Electronic Medical Record/IS Platform

- Concentra Electronic Health Record (EHR)

EXHIBIT B
PROGRAM FEES (“FEES”)

| Estimated Start-up Costs | | 1/2/2025 - 1/1/2026 | 1/2/2026 - 1/1/2027 |
|---|---------------|--------------------------------|--------------------------------|
| Furniture, Fixtures, & Equipment (FF&E) (<i>pass through</i>) | | As Incurred | \$0 |
| Network Installation (<i>pass through</i>) | | \$12,300 | \$0 |
| Data Feed Configuration | | \$2,500 | \$0 |
| Technology/Software Installation | | \$25,300 | \$0 |
| Implementation Fee | | \$7,300 | \$0 |
| Implementation Team Travel (<i>pass through</i>) | | As Incurred | \$0 |
| TOTAL START-UP COSTS | | \$47,400 | \$0 |
| Estimated Labor Fees (Staffing) | Hourly | Monthly | Annual |
| Physician - 1 FTE | \$170.32 | \$29,522.53 | \$354,270 |
| Advanced Practice Clinician (NP/PA) - 1 FTE w Backfill | \$123.10 | \$21,337.62 | \$256,051 |
| Advanced Practice Clinician (NP/PA) - 0.5 FTE | \$112.14 | \$9,718.41 | \$116,621 |
| Medical Assistant - 1 FTE | \$40.58 | \$7,033.95 | \$84,407 |
| Medical Assistant/Radiological Technician - 2 FTE w/backfill | \$64.74 | \$22,441.98 | \$269,304 |
| Certified Health Educator/Dietician - 0.5 FTE | \$45.21 | \$3,918.07 | \$47,017 |
| TOTAL LABOR FEES | | \$93,973 | \$1,127,671 |
| Estimated Ongoing Fixed Fees | | Monthly | Annual |
| Hardware Use Fee | | \$708.33 | \$8,500 |
| Software Fee | | \$2,083.33 | \$25,000 |
| Management Fee | | \$24,432.50 | \$293,190 |
| TOTAL ONGOING FIXED FEES | | \$27,224 | \$326,690 |
| Estimated Pass-Through Costs | | Monthly | Annual |
| Internet Network Connectivity | | As Incurred | As Incurred |
| Medical Supplies | | \$3,550.00 | \$42,600 |
| Laboratory | | \$4,678.32 | \$56,140 |
| Phone/Office Supplies/Admin/Travel/Other | | \$1,598.15 | \$19,178 |
| TOTAL PASS-THROUGH COSTS | | \$9,826.47 | \$117,918 |
| TOTAL ESTIMATED YEAR 1 COSTS | | \$1,619,678 | \$1,621,805 |

1. The table above is based on current estimates of scope and volume
 - (a) Any scope or volume changes may require additional Fees by amendment to this Agreement
2. Start Up Fees
 - (a) The actual one-time Fee for supply and equipment will be dependent upon the facility size and configuration
 - i. Items purchased will be passed through as incurred
 - (b) Implementation Fee to be billed upon executed Letter of Intent or execution of this Agreement, whichever comes first
 - (c) Staffing will begin up to thirty (30) days prior to the Onsite Center opening and will be billed as incurred until Onsite Center opening day.
 - (d) Implementation is anticipated to be finalized within ninety (90) days of the implementation commencing. The parties agree that implementation is considered complete on the date the Onsite Center is open for business
 - (e) Please note the amounts applied for recruiting are estimated, actual cost may vary, and estimate does not include placement cost from a recruiting agency
 - i. If deemed necessary, will be passed through to Client at cost
3. Concentra will bill ongoing labor, technology, and management fees to the Client as a flat monthly fee at 1/12 of the annual rate

- i. If deemed necessary, will be passed through to Client at cost
3. Concentra will bill ongoing labor, technology, and management fees to the Client as a flat monthly fee at 1/12 of the annual rate
 - (a) Concentra's standard payment terms are net thirty (30) days
 - (b) {only if not included in MSA above} On the earlier of (i) the beginning of each twelve (12) month period after the Effective Date of this Agreement; or (ii) on the anniversary of the commencement date of the existing Agreement between the parties (if applicable), all the Fees provided in the table above (excluding the pass-through items) shall automatically increase three percent 3%
 - (c) If additional hours are deemed temporarily necessary for existing staff members and/or staff roles that are not overtime hours, they will be billed as incurred at the hourly rates listed above in addition to the Monthly Fixed Fees
 - (d) If the checkbox for Back-fill above is checked "Yes":
 - i. The hourly charge for Back-fill for that position is included in the Monthly Fee above
 - (e) If the checkbox for Back-fill above is checked "No":
 - i. If Back-fill is provided anyway upon mutual agreement of the parties, then the hourly rate shown above shall be billed as incurred in addition to the Monthly Fee for that position
 - ii. Client shall be responsible for paying the fixed monthly fees while Concentra employees are out of the office on PTO, FMLA, or bereavement
 - (f) The fixed Monthly Fees shall be paid even if the clinic location is inaccessible due to temporary shutdowns and Client recognized holidays
4. Technology Fees include:
 - (a) Software fees (subject to change based on changes to staffing model)
 - (b) EMR Hardware Fee (all hardware purchases, maintenance of hardware, and replacement of hardware items necessary to provide the EMR solution, but excluding consumables)
 - (c) Patient survey
 - (d) Standard quarterly stewardship reporting
 - i. If customized reporting is requested by Client and is mutually agreed upon, then that customized reporting would be created by Concentra and billed on a time and materials basis at a rate of \$75 per hour of Concentra developer time spent in its creation and ongoing delivery.
 - (e) One standard data feed has been included in the above Fees for eligibility files. If Client requires additional feeds, then additional Fees shall apply:
 - i. If the desired data feed matches our standard layout, each additional feed would be \$2,500.00.
 - ii. If customized feeds are requested by Client (i.e. insurance carriers, etc.), then that customized feed would be created by Concentra and billed on a time and materials basis at a rate of \$75 per hour of Concentra developer time spent in its creation.
5. All other costs will be passed through as incurred
 - (a) Travel and mileage (at the current applicable IRS rate) expenses incurred in the performance of required services (including but not limited to clinical and physician travel, travel between Client locations, onsite staff travel for training, monthly meetings, mutually agreed agency expenses that may be incurred during any Term, quarterly stewardship meetings, audits, any Back-fill and colleague performance management) will be billed back at actual cost without additional markup or management fee (in accordance to FBC AnnexB Travel Policy)
 - (b) All consumable items necessary for day to day clinic operation, whether requested by client or deemed medically or operationally necessary by clinic staff, will be passed through to client as incurred without markup
 - i. Passed through items include, but are not limited to: medical supplies, office supplies, laboratory fees and supplies, shipping of specimens, break room supplies, printing, postage, parking fees, uniforms, , equipment calibration and maintenance, biohazard disposal, cell phones and data plans, third party services such as MROs or X-ray over reads if necessary, etc.
 - (c) Any change in scope to the Agreement that require certifications to be in compliance (CAOHC, BAT, UDS, DOT, etc.), and any travel related to this training will be passed through to Client as incurred
6. In addition to the fees listed in Exhibit B above, the Parties agree that Contractor will contract with a third-party vendor to provide the reasonable suspicion drug testing outside of clinic hours/overnight between the hours of 6pm-7am and the costs for those services will be a pass-through expense from Contractor to County for reimbursement to Contractor. The fees per collection are included below are guaranteed through January 2, 2027.
 - Onsite Fee (includes two hours) \$ 500.00
 - Each additional hour \$ 75.00
 - Drug Screen Collection Fee \$ 30.00
 - Drug Screen Fee \$ 50.00
 - Breath Alcohol/Blood Alcohol \$ 65.00
 - Mileage Current IRS Rate (www.irs.gov)

EXHIBIT C:
RFP 25-002

COUNTY PURCHASING AGENT
Fort Bend County, Texas



Jaime Kovar
County Purchasing Agent

(281) 341-8640
Fax (281) 341-8645

June 20, 2024

TO: All Prospective Respondents

RE: Addendum No.1 – Fort Bend County RFP 25-002 – Employee Health and Wellness
Clinical Services

Addendum 1:

Addendum 1 has been posted to the County’s website. Vendors are to use the Addendum 1 file while preparing their proposal. The due date has been extended to 7/2/24 @ 2:00 PM, see 31.4, 38.0 and 40.0. Also, see Q&A 1 and 2 documents posted on the FBC website.

Immediately upon your receipt of this addendum, please fill out the following information and email this page to Olivia Rios at Olivia.Rios@fortbendcountytexas.gov .

Company Name

Signature of person receiving addendum

Date

If you have any questions, please contact this office.

Sincerely,

Cheryl Krejci
Assistant County Purchasing Agent

***Amended, 6/21/24**
Fort Bend County, Texas
Request for Proposals



Employee Health and Wellness Clinical Services
RFP 25-002

SUBMIT SEALED PROPOSALS TO:

Fort Bend County
Purchasing Department
Travis Annex
301 Jackson, Suite 201
Richmond, TX 77469

Note: All correspondence must include the term
“Purchasing Department” in address to assist in
proper delivery.

***SUBMIT NO LATER THAN:**

*Tuesday, July 2 ~~June 25~~, 2024
2:00 PM (Central)

LABEL SEALED ENVELOPE/BOX:

RFP 25-002
EMPLOYEE CLINICAL SERVICES

***ALL RFPs MUST BE RECEIVED IN AND TIME/DATE STAMPED BY THE PURCHASING OFFICE
OF FORT BEND COUNTY ON OR BEFORE THE SPECIFIED TIME/DATE STATED ABOVE.***

RFPs RECEIVED AS REQUIRED WILL THEN BE OPENED AND NAMES PUBLICLY READ.

RFPs RECEIVED AFTER THE SPECIFIED TIME, WILL BE RETURNED UNOPENED.

Result will be provide, upon request,
after final agreement is approved by
Commissioners Court.

Requests for information must be in
writing and directed to:
Cheryl Krejci, CPPB
Assistant County Purchasing Agent
Cheryl.Krejci@fortbendcountytexas.gov

Vendor Responsibilities:

- Download and complete any addendums. (Addendums will be posted on the Fort Bend County website no Later than 48 hours prior to bid opening)
- Submit response in accordance with requirements stated on the cover of this document.
- DO NOT submit responses via email or fax.



**COUNTY PURCHASING AGENT
Fort Bend County, Texas**

Vendor Information

Jaime Kovar
Purchasing Agent

Office (281) 341-8640

| | | | |
|--|--|---|------------------------------|
| Legal Company Name (top line of W9) | Concentra Health Services, Inc. | | |
| Business Name (if different from legal name) | dba Concentra Medical Centers | | |
| Type of Business | <input checked="" type="checkbox"/> Corporation/LLC <input type="checkbox"/> Sole Proprietor/Individual | <input type="checkbox"/> Partnership <input type="checkbox"/> Tax Exempt | Age in Business? 45 years |
| Federal ID # or S.S. # | 75-2510547 | SAM.gov Unique Entity ID # | S5D7ZCRVME35 |
| SAM.gov CAGE / NCAGE | 1QX60 | | |
| Publicly Traded Business | ___ No | <u>X</u> Yes | Ticker Symbol <u>SEM</u> |
| Remittance Address | P.O. Box 9005 | | |
| City/State/Zip | Addison, TX 75001 | | |
| Physical Address | 5080 Spectrum Drive, #1200W | | |
| City/State/Zip | Addison, TX 75001 | | |
| Phone Number | 972.364.8000 | | |
| E-mail | ergerber@concentra.com | | |
| Contact Person | Erica Gerber, Director of Onsite Sales | | |
| Check all that apply to the company listed above and provide certification number. | DBE-Disadvantaged Business Enterprise <input type="checkbox"/> | Certification # _____ | <u>Cert Date</u> _____ |
| | SBE-Small Business Enterprise <input type="checkbox"/> | Certification # _____ | <u>Exp Date</u> _____ |
| | HUB-Texas Historically Underutilized Business <input type="checkbox"/> | Certification # _____ | _____ |
| | WBE-Women's Business Enterprise <input type="checkbox"/> | Certification # _____ | _____ |
| Company's gross annual receipts | <\$500,000 _____ | \$500,000-\$4,999,999 _____ | |
| | \$5,000,000-\$16,999,999 _____ | \$17,000,000-\$22,399,999 _____ | >\$22,400,000 <u>X</u> |
| NAICs codes (Please enter all that apply) | 62111 | | |
| Signature of Authorized Representative | DocuSigned by: 03C65E7A36BF425... | | |
| Printed Name | Mike Rhine | | |
| Title | EVP, COO, Concentra Health Services, Inc. | | |
| Date | 06/21/2024 | | |

THIS FORM MUST BE SUBMITTED WITH THE SOLICITATION RESPONSE

Fort Bend County RFP 25-002

1.0 INTRODUCTION:

Fort Bend County, Texas (hereafter referred to as the (“County”)) seeks sealed Proposals (“Proposals or RFP”) from qualified firms seeking to offer on-site medical services (“Project”) to its employees, retirees and dependents. Respondents must offer a proposal that will meet the scope of services, qualifications and general description of work activities identified in the RFP.

2.0 GUIDELINES:

By virtue of submitting a proposal, interested parties are acknowledging:

- 2.1 The County reserves the right to reject any or all proposals if it determines that select proposals are not responsive to the RFP. The County reserves the right to reconsider any proposal submitted at any phase of the procurement. It also reserves the right to meet with select Respondents at any time to gather additional information. Furthermore, the County reserves the right to delete or add scope up until the final contract signing.
- 2.2 All Respondents submitting proposals agree that their pricing is valid for a minimum of ninety (90) days after proposal submission to the County. Furthermore, the County is by statute exempt from the State Sales Tax and Federal Excise Tax; therefore, proposal prices shall not include taxes.
- 2.3 This Proposal does not commit the County to award nor does it constitute an offer of employment or a contract for services. Costs incurred in the submission of this proposal, or in making necessary studies or designs for the preparation thereof, are the sole responsibility of the Respondents. Further, no reimbursable cost may be incurred in the anticipation of award. Proposals containing elaborate artwork, expensive paper and binding and expensive visual or other presentations are neither necessary nor desired.
- 2.4 In an effort to maintain fairness in the process, all inquiries concerning this procurement are to be directed only to the County’s Purchasing Agent in writing. Attempts to contact any members of the County’s Commissioners’ Court or any other County employee to influence the procurement decision may lead to immediate elimination from further consideration.
- 2.5 When responding to this Proposal, follow all instructions carefully. Submit proposal contents according to the outline specified and submit all hard copy and electronic documents according to the instructions. Failure to follow these instructions may be considered a non-responsive proposal and may result in immediate elimination from further consideration.

Fort Bend County RFP 25-002

3.0 PROPOSAL CONTACT:

This Proposal is being issued by the County Purchasing Agent on behalf of Fort Bend County, Texas. Thus, responses should be directed to the Assistant Purchasing Agent, as outlined below. **Respondents are specifically directed NOT to contact any County personnel for meetings, conferences or technical discussions that are related to this Proposal other than specified herein. Unauthorized contact of any County personnel will likely be cause for rejection of the Respondent’s proposal. All communications regarding the Proposal shall be directed to the County’s Proposal Contact.** Communication with the Proposal Contact is permitted via email or written correspondence.

PROPOSAL CONTACT:

Cheryl Krejci, CPPB
Assistant County Purchasing Agent
Fort Bend County Travis Annex
301 Jackson, Suite 201
Richmond, Texas 77469
Cheryl.Krejci@fortbendcountytexas.gov

***4.0 SUBMISSION REQUIREMENTS:**

4.1 Submission requirements: one (1) original proposal, ten (10) paper copies, and one (1) electronic response on a labeled flash drive are required by RFP opening time of **2:00 PM on Tuesday, July 2 ~~June 25~~, 2024**. Flash drive must contain only one (1) file in PDF format and must match written/original/paper response identically. Failure to provide proper original, flash drive or copies is cause for disqualification. Proposal shall be submitted to the address shown below. Proposal shall be signed by a person having the authority to bind the firm in a contract.

| | |
|------------------------|---|
| Fort Bend County | Proposal Number: R25-002 |
| Purchasing Department | Due Date: Tuesday, July 2 June 25 , 2024 |
| 301 Jackson, Suite 201 | Time: 2:00 PM (CST) |
| Richmond, TX 77469 | For: Employee Health & Wellness Clinical Services |

4.2 Respondents may submit their proposal any time prior to the Opening Date and time after confirmation of addendum status. The Respondent’s name and address as well as a distinct reference to the Proposal number above shall be marked clearly on the submission. All proposals are time-stamped upon receipt and are securely kept, unopened, until the Opening Date. No responsibility will attach to the County, or any official or employee thereof, for the pre-opening of, post-opening of, or the failure to open a proposal not properly addressed and identified. No oral, telegraphic, telephonic, emailed or facsimile proposals will be considered.

4.3 Proposals may be modified or withdrawn prior to the established opening date by delivering written notice to the proposal contact. Any alteration made prior to

Fort Bend County RFP 25-002

opening date and time shall be initialed by the signer of the proposal, guaranteeing authenticity.

- 4.4 Proposals time-stamped after the due date and time will not be considered and will be returned to the Respondent unopened. Regardless of the method used for delivery, respondents shall be wholly responsible for the timely delivery of submitted proposals.
- 4.5 The Respondent's name and address shall be clearly marked on all copies of the proposal.

5.0 INCURRED COSTS:

Those submitting proposals do so entirely at their expense. There is no expressed or implied obligation by the County to reimburse any individual or firm for any costs incurred in preparing or submitting proposals, for providing additional information when requested by the County or for participating in any selection interviews, including discovery (pre-contract negotiations) and contract negotiations.

6.0 ACCEPTANCE:

- 6.1 Submission of any proposal indicates a Respondent's acceptance of the conditions contained in this Proposal unless clearly and specifically noted otherwise in their proposal.
- 6.2 Furthermore, the County is not bound to accept a proposal on the basis of lowest price, and further, the County has the sole discretion and reserves the right to cancel this Proposal, to reject any and all proposals, to waive any and all informalities and or irregularities, or to re-advertise with either the identical or revised specifications, if it is deemed to be in the County's best interests. The County reserves the right to accept or reject any or all of the items in the proposal, and to award the contract in whole or in part and/or negotiate any or all items with individual Respondents if it is deemed in the County's best interest.
- 6.3 Although Fort Bend County desires to negotiate toward a contract with a selected Respondent, the Commissioners' Court may award the contract on the basis of the initial proposals received, without discussions. Therefore, each initial proposal should contain the Respondent's best terms.

7.0 INTERPRETATIONS, DISCREPANCIES, AND OMISSIONS:

- 7.1 It is incumbent upon each potential Respondent to carefully examine these specifications, terms, and conditions. Should any potential Respondent find discrepancies, omissions or ambiguities in this Proposal, the Respondent shall at once request in writing an interpretation from the County's Proposal Contact. Any inquiries, suggestions, or requests concerning interpretation, clarification or

Fort Bend County RFP 25-002

additional information shall be made in writing via e-mail only to the County's Proposal Contact, as specified in Section 3.0. Deadline for submission of questions and/or clarification is no later than **Monday, June 10, 2024 at 9:00AM (CST)**. Requests received after the deadline will not be responded to due to the time constraints of this Proposal process.

- 7.2 The issuance of a written addendum is the only official method by which interpretation, clarification or additional information will be given by the County. Only questions answered by formal written addenda will be binding. Oral and other interpretations or clarification will be without legal effect. If it becomes necessary to revise or amend any part of this Proposal, notice will be given by the County Purchasing Agent to all prospective Respondents who were sent a Proposal. The Respondent in their proposal shall acknowledge receipts of amendments. Each Respondent shall ensure that they have received all addenda and amendments to this Proposal before submitting their proposals.

8.0 CONTRACTUAL OBLIGATIONS:

This Request for Proposal, response and associated documentation, any negotiations and final contract, when properly accepted by Fort Bend County, shall constitute a contract equally binding between the contractor and Fort Bend County.

9.0 RETENTION OF RESPONDENT'S MATERIAL:

The County reserves the right to retain all proposals regardless of which response is selected. All proposals and accompanying documents become the property of the County.

10.0 ASSIGNMENT:

The Respondent may not sell, assign, transfer or convey the contract resulting from this Proposal, in whole or in part, without the prior written approval from Fort Bend County Commissioners' Court.

11.0 CERTIFICATE OF INDEPENDENT PRICE DETERMINATION:

By submission of a proposal, each Respondent certifies, that in connection with this procurement:

- 11.1 The prices in this proposal have been arrived at independently, without consultation, communication, or agreement with any other Respondent; with any competitor; or with any County employee(s) or consultant(s) for the purpose of restricting competition on any matter relating to this Proposal.
- 11.2 Unless otherwise required by law, the prices which have been quoted in this proposal have not been knowingly disclosed by the Respondent and will not knowingly be disclosed by the Respondent prior to award directly or indirectly to any other Respondent or to any competitor; and;

Fort Bend County RFP 25-002

- 11.3 No attempt has been made or will be made by the Respondent to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

12.0 CONFIDENTIAL MATTERS:

- 12.1 All data and information gathered by the Respondent and its agents, including this Proposal and all reports, recommendations, specifications, and data shall be treated by the Respondent and its agents as confidential. The Respondent and its agents shall not disclose or communicate the aforesaid matters to a third party or use them in advertising, publicity, propaganda, and/or in another job or jobs, unless written consent is obtained from the County.
- 12.2 Proposals will only be publicly received and acknowledged only so as to avoid disclosure of the contents to competing Respondents and kept secret during negotiation. However, all proposals shall be open for public inspection after the contract is awarded. Trade secrets and any material that is considered to be confidential information contained in the proposal and identified by Respondent as such will be treated as confidential to the extent allowable in the Open Records Act.

13.0 LIMITS OF SUBCONTRACTORS:

- 13.1 The County has approval rights over the use and/or removal of all subcontractors and/or vendor(s). Subcontractors shall conform to all County policies.
- 13.2 Any dispute between the Respondent and subcontractors, including any payment dispute, will be promptly remedied by the Respondent. Failure to promptly remedy or to make prompt payment to subcontractor may result in the withholding of funds from the Respondent by the County for any payments owed to the subcontractor.

14.0 JURISDICTION, VENUE, CHOICE OF LAW:

This Proposal and any contract resulting there from shall be governed by and construed according to the laws of the State of Texas. Should any portion of any contract be in conflict with the laws of the State of Texas, the State laws shall invalidate only that portion. The remaining portion of the contract(s) shall remain in effect. Any lawsuit shall be governed by Texas law and Fort Bend County, Texas shall be the venue for any action or proceeding that may be brought or arise out of, in connection with or by reason of this Proposal process and resulting Agreements.

15.0 INDEPENDENT CONTRACTOR:

The Respondent is an independent contractor and no employee or agent of the Respondent shall be deemed for any reason to be an employee or agent of the County.

Fort Bend County RFP 25-002

16.0 AMERICANS WITH DISABILITIES ACT (ADA)

Proposals shall comply with all federal, state, county, and local laws concerning this type of products/service/equipment/project and the fulfillment of all ADA requirements.

17.0 DRUG-FREE WORKPLACE:

All Respondents shall provide any and all notices as may be required under the Drug-Free Workplace Act of 1988, 28 CFR Part 67, Subpart F, to their employees and all sub-contractors to insure that the County maintains a drug-free workplace.

18.0 PERFORMANCE AND PAYMENT BOND:

No performance nor payment bond is required for this project.

19.0 POWER OF ATTORNEY:

An attorney-in-fact who signs a bid bond, performance bond or payment bond must file with each bond a certified and effectively dated copy of his or her power of attorney.

20.0 TEXAS ETHICS COMMISSION FORM 1295:

20.1 Effective January 1, 2016 all contracts executed by Commissioners Court, regardless of the dollar amount, will require completion of Form 1295 “Certificate of Interested Parties”, per the new Government Code Statute §2252.908. All firms submitting a response to a formal Bid, RFP, SOQ or any contracts, contract amendments, renewals or change orders are required to complete the Form 1295 online through the State of Texas Ethics Commission website. Please visit:

<https://www.ethics.state.tx.us/File/>

20.2 On-line instructions:

20.2.1 Name of governmental entity is to read: Fort Bend County.

20.2.2 Identification number use: RFP 25-002.

20.2.3 Description is: Employee Health & Wellness Clinical Services.

20.3 Highest evaluated vendor will be required to provide the Form 1295 within three (3) calendar days from notification; however, if your company is publicly traded you are not required to complete this form.

Fort Bend County RFP 25-002

21.0 INSURANCE:

- 21.1 All respondents shall submit, with RFP, a current certificate of insurance indicating coverage in the amounts stated below. In lieu of submitting a certificate of insurance, respondents may submit, with RFP, a notarized statement from an Insurance company, authorized to conduct business in the State of Texas, and acceptable to Fort Bend County, guaranteeing the issuance of an insurance policy, with the coverage stated below, to the firm named therein, if successful, upon award of this Contract.
- 21.2 At contract execution, contractor shall furnish County with properly executed certificates of insurance, which shall evidence all insurance required and provide that such insurance shall not be canceled, except on 30 days prior written notice to County. Contractor shall provide certified copies of insurance endorsements and/or policies if requested by County. Contractor shall maintain such insurance coverage from the time Services commence until Services are completed and provide replacement certificates, policies and/or endorsements for any such insurance expiring prior to completion of Services. Contractor shall obtain such insurance written on an Occurrence form (or a Claims Made form for Professional Liability insurance) from such companies having Best's rating of A/VII or better, licensed or approved to transact business in the State of Texas, and shall obtain such insurance of the following types and minimum limits:
- 21.2.1 Workers' Compensation insurance. Substitutes to genuine Workers' Compensation Insurance will not be allowed.
- 21.2.2 Employers' Liability insurance with limits of not less than \$1,000,000 per injury by accident, \$1,000,000 per injury by disease, and \$1,000,000 per bodily injury by disease.
- 21.2.3 Commercial general liability insurance with a limit of not less than \$1,000,000 each occurrence and \$2,000,000 in the annual aggregate. Policy shall cover liability for bodily injury, personal injury, and property damage and products/completed operations arising out of the business operations of the policyholder.
- 21.2.4 Professional (Medical Malpractice) Liability Insurance: Medical Malpractice Liability Insurance shall be maintained with limits of no less than \$1,000,000 per occurrence and \$3,000,000 in aggregate.
- 21.3 County and the members of Commissioners Court shall be named as additional insured on a Primary and Non-Contributory basis to all required coverage except for Workers' Compensation and Professional Liability (Medical Malpractice) Insurance. All Liability policies including Workers' Compensation written on behalf of contractor, shall contain a waiver of subrogation in favor of County and members of Commissioners Court.

Fort Bend County RFP 25-002

- 21.4 If required coverage is written on a claims-made basis, contractor warrants that any retroactive date applicable to coverage under the policy precedes the effective date of the contract; and that continuous coverage will be maintained or an extended discovery period will be exercised for a period of two (2) years beginning from the time that work under the agreement is completed.

22.0 INDEMNIFICATION:

Respondent shall save harmless County from and against all claims, liability, and expenses, including reasonable attorney's fees, arising from activities of Respondent, its agents, servants or employees, performed under this agreement that result from the negligent act, error, or omission of Respondent or any of Respondent's agents, servants or employees.

- 22.1 Respondent shall timely report all such matters to Fort Bend County and shall, upon the receipt of any such claim, demand, suit, action, proceeding, lien or judgment, not later than the fifteenth day of each month; provide Fort Bend County with a written report on each such matter, setting forth the status of each matter, the schedule or planned proceedings with respect to each matter and the cooperation or assistance, if any, of Fort Bend County required by Respondent in the defense of each matter.
- 22.2 Respondent's duty to defend, indemnify and hold Fort Bend County harmless shall be absolute. It shall not abate or end by reason of the expiration or termination of any contract unless otherwise agreed by Fort Bend County in writing. The provisions of this section shall survive the termination of the contract and shall remain in full force and effect with respect to all such matters no matter when they arise.
- 22.3 In the event of any dispute between the parties as to whether a claim, demand, suit, action, proceeding, lien or judgment appears to have been caused by or appears to have arisen out of or in connection with acts or omissions of Respondent, Respondent shall never-the-less fully defend such claim, demand, suit, action, proceeding, lien or judgment until and unless there is a determination by a court of competent jurisdiction that the acts and omissions of Respondent are not at issue in the matter.
- 22.4 Respondent's indemnification shall cover, and Respondent agrees to indemnify Fort Bend County, in the event Fort Bend County is found to have been negligent for having selected Respondent to perform the work described in this request.
- 22.5 The provision by Respondent of insurance shall not limit the liability of Respondent under an agreement.
- 22.6 Respondent shall cause all trade contractors and any other contractor who may have a contract to perform construction or installation work in the area where work will be performed under this request, to agree to indemnify Fort Bend County and to hold it harmless from all claims for bodily injury and property damage that arise

Fort Bend County RFP 25-002

may from said Respondent's operations. Such provisions shall be in form satisfactory to Fort Bend County.

22.7 Loss Deduction Clause - Fort Bend County shall be exempt from, and in no way liable for, any sums of money which may represent a deductible in any insurance policy. The payment of deductibles shall be the sole responsibility of Respondent and/or trade contractor providing such insurance.

23.0 STATE LAW REQUIREMENTS FOR CONTRACTS:

The contents of this section are required by Texas Law and are included by County regardless of content.

23.1 Agreement to Not Boycott Israel Chapter 2271 Texas Government Code: Contractor verifies that if Contractor employs ten (10) or more full-time employees and this Agreement has a value of \$100,000 or more, Contractor does not boycott Israel and will not boycott Israel during the term of this Agreement.

23.2 Texas Government Code Section 2251.152 Acknowledgment: By signature on vendor form, Contractor represents pursuant to Section 2252.152 of the Texas Government Code, that Contractor is not listed on the website of the Comptroller of the State of Texas concerning the listing of companies that are identified under Section 806.051, Section 807.051 or Section 2253.153.

24.0 HUMAN TRAFFICKING:

By acceptance of this contract, Contractor acknowledges that Fort Bend County is opposed to human trafficking and that no County funds will be used in support of services or activities that violate human trafficking laws.

***25.0 TENTATIVE SCHEDULE:**

| | |
|--|---|
| Release of RFP: | May 26, 2024 |
| Pre-RFP Conference and Site Visit: | June 4, 2024, 9:00 AM |
| Deadline for Questions: | June 10, 2024, 9:00 AM |
| Submission Due Date: | July 2 June 25 , 2024, 2:00 PM |
| Evaluation of Submissions: | Week of July 8, 2024 |
| Commissioners Court Permission to Negotiate: | July 23, 2024 |
| Negotiations: | Begin July 24, 2024 |
| Final Contract Approval Commissioners Court: | September 10, 2024 |

26.0 PRE-RFP CONFERENCE AND SITE VISIT:

A pre-RFP conference and site visit will be conducted on **Tuesday, June 4, 2024 at 9:00AM (CST)**. The pre-RFP conference will be held at the Fort Bend County Purchasing Department located at 301 Jackson, Suite 201, Richmond, Texas. A site-visit will be held immediately

Fort Bend County RFP 25-002

following the conference. Attendance is not mandatory; however, all firms are encouraged to attend.

27.0 DETAILED SCOPE OF WORK:

27.1 The following services shall be provided to the County to include, but not limited to the following:

- 27.1.1 Primary care
- 27.1.2 Urgent care (including casting)
- 27.1.3 Biometric testing/Health risk assessments and active wellness program
- 27.1.4 Nicotine cessation
- 27.1.5 Weight loss
- 27.1.6 Mental health
- 27.1.7 Call support
- 27.1.8 Immunizations
- 27.1.9 Injections
- 27.1.10 New hire physicals
- 27.1.11 Pre-employment and post accident drug testing with MRO service
- 27.1.12 Sports physicals
- 27.1.13 Annual well-woman/well-man exams
- 27.1.14 DOT medical exams
- 27.1.15 Prescriptions/Formulary
- 27.1.16 Pharmaceuticals
- 27.1.17 Disease management
- 27.1.18 Primary care case management
- 27.1.19 Worker's compensation treatment and coordination with temporary transitional assignment program

Fort Bend County RFP 25-002

- 27.1.20 Post-accident drug test collection
- 27.1.21 Blood-borne/airborne pathogen testing
- 27.1.22 Radiology
- 27.1.23 Quick test labs

27.2 In addition to on-site healthcare, the County requires on-site medical services to include providing health risk assessments (HRA). The County requires disease management services driven by HRAs and/or its health plans, medical and pharmacy claims data, so it can reach members who don't access the clinic. The provider will work with the County to establish/maintain a wellness program to provide educational, intervention and incentive programs. The provider must have software capabilities that will allow integration to Third Party Administrators who provide claims adjudication services for the County health plan and the workers compensation program. The provider must also have software capabilities that will allow interfacing with the County system. The provider will coordinate services with the medical plan, workers compensation plan, E.A.P program and any pre-certification program utilized by the County medical program or workers compensation program. The provider must comply with Texas Health and Safety Code, Chapter 181, Medical Privacy and all guidelines and regulations set forth in the Health Insurance Portability and Accountability Act (H.I.P.A.A.) and will be required to sign an H.I.P.A.A. Business Associate Agreement with the County.

28.0 PRIMARY CARE:

- 28.1 On-line appointment scheduling must be available.
- 28.2 Describe the types of problems/medical conditions that can be addressed on-site.
- 28.3 Describe the medications to be administered on-site.
- 28.4 Physician(s) must have hospital privileges in Fort Bend County area hospitals. Provide list of hospitals.
- 28.5 Describe walk-in, sick call process.

29.0 WORKER'S COMPENSATION:

- 29.1 Describe the types of problems that can be addressed on-site.
- 29.2 What if a medical condition escalates?
- 29.3 Describe the role of the on-site physician in conjunction with Worker's Compensation injuries.

Fort Bend County RFP 25-002

29.4 Describe process for determining fitness for duty.

30.0 COMMUNICATION PLAN AND MEMBER SERVICES:

Provide a proposed communication plan for introducing onsite healthcare and wellness program and reference the ongoing communication process. Outline your company's responsibilities in these processes. Include copies of your educational materials and timelines for distribution.

30.1 How can employees, retirees and dependents communicate with the medical team?

30.2 How many average patients should be expected to be treated in an hour per medical provider?

30.3 Will you utilize existing resources for clinic?

30.4 What staffing do you envision?

30.5 What days and hours of operation do you recommend (including walk-in and sick call program)? Currently our clinic hours are 7:00 AM – 5:00 PM, Monday through Friday. The County is interested in extending Monday through Friday hours to 7:00 AM - 6:00 PM. The County is also interested in an option to be open on Saturdays, 8:00 AM through 4:00 PM. Include pricing with and without Saturday hours in your proposal.

30.6 Describe your availability to provide health care on nights and weekends.

30.7 Is your health risk assessment available both on-line and off-line?

30.8 Can your website be linked with the County's website?

30.9 Describe your ability to communicate with an employee, retiree and dependent population that is geographically dispersed. Provide examples.

30.10 Discuss the frequency and type of communications that eligible persons will receive throughout the program period.

30.11 How can an employee, retiree or dependent access your company for Member Services after hours?

30.12 Provide your web address and any access codes needed to explore your services.

30.13 Are you willing for County to use its own branding in communication and program materials?

30.14 Do you provide a 24 hour nurse on-call?

Fort Bend County RFP 25-002

***31.0 ADDITIONAL INFORMATION:**

- 31.1 Mental Health Services-Clinic screens for mental health problems and provides mental health care within the scope of Primary Care (i.e.; anxiety and depression). For more complicated issues, clinicians refer to the EAP for access to counseling and/or psychiatry.
- 31.2 Current operating business partner of the clinic is Next Level Health & Wellness.
- 31.3 The clinic facility, furnishings, equipment and supplies are owned by or provided by Fort Bend County.
- *31.4 Clinic staff currently consists of one (1) part-time physician (16 hours in clinic and 4 hours of oversight of APPS), two (2) physician assistants (one (1) APP works 30 hours per week and the other APP works 20 hours per week), and three (3) full-time medical assistants (at least one (1) must be a certified radiology technician). County is interested in having a minimal of 40 hours of physician clinical service and a minimal of 60 hours of APP clinical service.
~~Clinic staff currently consists of one (1) full-time physician, two (2) physician assistants, and three (3) medical assistants (at least one must be a certified radiology technician).~~
- 31.5 Clinic has its' own x-ray equipment. The equipment is a AMRAD Advantage FRS System with Viewworks Fixed 17 x 17 GADOX DR Panel.
- 31.6 Images are transmitted via software to a Radiologist for interpretation. The Radiologist charges a fee that is a pass-through fee to FBC.
- 31.7 Pass-through costs for the Clinic include Radiologist charges, supplies, & quick-test labs.
- 31.8 Marketing/Communication for the Clinic is provided by the FBC Risk Management Department.
- 31.9 The clinic provides wellness services including nicotine cessation, weight loss, vaccinations, biometric and Health Risk Assessments.
- 31.10 The clinic is a FBC property located at 301 Jackson Street, Richmond, TX.
- 31.11 The clinic has a waiting room, three offices, six exam rooms, a supply room, radiology room, minor procedure medical surgical room, lab, lab collection restroom, restroom and buildout for potential future pharmacy which is currently being used for extra storage space.
- 31.12 Plan participant dependents may be treated in the Clinic beginning at five (5) years of age.

Fort Bend County RFP 25-002

- 31.13 The clinic does perform youth physicals.
- 31.14 No audiometric screening booth is onsite.
- 31.15 For industrial accident injuries, FBC Workers Compensation business partner is Davies-Group.
- 31.16 The clinic provides drug testing services for pre-employment and post-accident. Breath Alcohol Testing is also performed.
- 31.17 FBC's Pharmaceutical Manager is CVS-Caremark.
- 31.18 The County's medical program is a self-insured program; administered by Boon Chapman.
- 31.19 FBC's Employee Assistance Program contractor is Deer Oaks.
- 31.20 The clinic provider is currently using Touchworks and AllScript for EMR.
- 31.21 Telemedicine is not currently provided by the clinic operator. However, as a separate benefit of services for plan participants, FBC does offer telemedicine through TeleDoc.

32.0 ADDITIONAL SERVICES:

Describe any additional services your company can provide including any additional costs for these services (i.e.; ability to provide telemedicine or satellite office(s) for onsite medical care equal to those of the employee clinic).

33.0 IDENTIFICATION OF HIGH RISK INDIVIDUALS:

Understanding that there are a variety of methodologies for implementing an HRA/targeted intervention process, please explain, in detail, the HRA/targeted intervention model that your organization would recommend. Explain the rationale behind your recommendation. The process must be confidential following all H.I.P.A.A. guidelines. How would your company identify high-risk members?

- 33.1 Describe your methodology for tracking and intervening with high risk members on an on-going basis.
- 33.2 Do you stratify members by severity of risk for complication? Please elaborate.
- 33.3 What Health Risk Assessment (HRA) do you use and how long have you used it? List all risk factors you identify in your profile. Please provide a sample HRA in your response.

Fort Bend County RFP 25-002

- 33.4 How often do you recommend that the members have an HRA?
- 33.5 Describe turnaround time for each of the following areas:
 - 33.5.1 Providing the HRA results to individuals;
 - 33.5.2 Contacting individuals for possible interventions;
 - 33.5.3 Providing County with a summary report of the initial HRA results.
- 33.6 Describe how your organization would provide a system to assist HRA participants' in completion of their questionnaires and in the interpretation of their personal profile.
- 33.7 Describe how your organization will set and reach participation goals?
- 33.8 Do you recommend using incentives? If so, please describe the incentives your organization recommends.
- 33.9 Describe your plan to involve new employees in the HRA process.
- 33.10 Describe your capabilities to update an individual's HRA record while conducting follow-up calls.
- 33.11 How does your HRA monitor and report individual change from year to year?

34.0 INTERVENTION:

Describe how to link to on-site or community programs (i.e. Employee Assistance Program, wellness screening, etc).

35.0 MEASUREMENT TOOLS AND RESULTS:

Provide a copy of your quality assurance program to include standards measurement criteria for onsite healthcare activities, costs, outcomes, HRA, disease management, member services, member intervention, and educational materials.

- 35.1 How would you propose measuring the outcomes and success of the overall program including a model Return on Investment (ROI)?
- 35.2 Describe your standard management reports. Describe your custom reporting capabilities and the associated costs. Provide a recommendation and examples of reports that you would provide the County.
- 35.3 Provide examples of the following:

Fort Bend County RFP 25-002

- 35.3.1 onsite healthcare activity report;
 - 35.3.2 HRA and member profile;
 - 35.3.3 member participation;
 - 35.3.4 member intervention;
 - 35.3.5 financial summary/savings report;
 - 35.3.6 Are management reports available online?
 - 35.3.7 Ad Hoc report capabilities.
- 35.4 Describe how your program specifically evaluates the effectiveness of primary care case management. Include any results of the evaluation as an attachment.
- 35.5 Provide all clinical indicators used to track the success of the program and the results, if any, by year since inception of the program.
- 35.6 Describe specifically how records for individuals with both personal health and job injury clinic experience will be managed.

36.0 HIPAA COMPLIANCE:

- 36.1 Is your firm H.I.P.A.A. compliant?
- 36.2 Describe your system for the assurance of personal health data security.
- 36.3 Have your network security systems ever been breached? If so, describe.
- 36.4 Include a copy of your H.I.P.A.A. Business Associate Agreement.

37.0 PROPOSED PROGRAM COSTS:

It is the County's intention to provide onsite health care and population health management services including health risk assessment to every employee, retiree and their dependents participating in our self-funded medical plan and all employees who are covered under our workers compensation program. Please include the following in your detailed pricing:

- 37.1 Staffing, including each doctor, consulting/specialty care;
- 37.2 Baseline fees, general administrative and operating costs;
- 37.3 Pharmaceuticals;

Fort Bend County RFP 25-002

- 37.4 Start-up costs/fees, bonds, insurance, supplies, misc. expenses;
- 37.5 Indicate all payment terms and conditions.

***38.0 EVALUATION CRITERIA:**

In order to facilitate the analysis of responses to this proposal, Respondents are required to prepare their proposals in accordance with the instructions outlined herein. Proposals should be prepared as simply as possible and provide a straightforward, concise description of the Respondent’s capabilities to satisfy the requirements of the proposal. Emphasis should be concentrated on accuracy, completeness, and clarity of content. All parts, pages, figures, and tables are required to be numbered, clearly labeled and tabbed with binder tabs/dividers for locating information quickly and easily. Font size below 12 point is prohibited.

- 38.1 Respondents are required to follow the outline below when preparing their proposals:

| Tab | Title |
|-----|---|
| | Title Page |
| | Table of Contents |
| | Executive Summary |
| 1 | Understanding scope of work |
| 2 | Firm experience |
| 3 | Staffing |
| 4 | Price |
| 5 | Required forms and overall completeness of submission |

- 38.2 Any exceptions to the Proposal requirements shall be identified in the applicable section in red type and referenced as numbered herein.
- 38.3 Executive Summary - This section should be limited to a brief narrative highlighting the company’s background and experience. Narrative should clearly demonstrate compliance with Respondent qualifications listed in the RFP specifications. Include length of time the company has been in business and provide examples of similar past projects.
- *38.4 Respondents will be evaluated utilizing the factors, as weighted below:

Tab 1

*Understanding Scope of Work (weight factor = 20 40%)

- Describe proposer’s understanding, responsiveness and approach to initiating and implementing the healthcare service program. Also include descriptions of:

Fort Bend County RFP 25-002

1. All healthcare service innovations respondent is proposing;
2. The effectiveness of the proposed healthcare services and how such effectiveness is measured;
3. All requested information as stated in Sections 27.0 through 36.0 referencing as numbered herein;
4. Any unique services or special expertise your healthcare firm offers that might bring value and/or efficiency to the County.

Tab 2

Firm Experience (weight factor = 20%)

- Firm Experience with Healthcare Services in a clinic setting of similar size:
 1. Identify the length of time the firm has been in business of providing onsite health care services in a clinic setting.
 2. Identify the current and/or past seven (7) years of performance in a similar nature to the performance offered in response to this RFP.
 3. Provide three (3) letters of recommendation, on reference provider's letterhead, regarding onsite healthcare, from entities the respondent has provided services for within the last seven (7) years, including company/entity name, physical address, contact person, phone number, and email address.
 4. Include a list of newly awarded contracts currently being implemented. Include for what entity/company and location.

Tab 3

Staffing (weight factor = 20%)

- Provide an organizational chart showing the level of organizational responsibility and the services provided by each of the members of your firm's proposed healthcare team. Include individual's resumes of those principals, partners and other key service staff members who will be directly involved in the overall service.

Tab 4

Price (weight factor = 20%)

- Provide itemized annual pricing for full performance in meeting the requirements of this RFP. Provide additional/optional service fees/costs separately.

Fort Bend County RFP 25-002

Tab 5

Required forms and overall completeness of submission (weight factor = 5%)

- Proof of Insurance
- Completed Respondent forms
- Completed W9 form
- Completed debt form

39.0 TERM OF CONTRACT:

The term of this contract is for a period of twenty-four (24) months, commencing on January 1, 2025, and ending at the close of business on December 31, 2026, with three (3) additional one-year renewal options under the same terms and conditions if mutually agreeable to both parties. Either party for any reason may terminate this contract by giving thirty (30) days written notice of the intent to terminate.

***40.0 AWARD:**

RFP will be evaluated by a committee comprised of County staff. The selection criteria totals eighty-five ~~seventy-five~~ (85 ~~75~~) percent, which will be utilized during the initial evaluation process. Once the short-list of firms, of no more than four (4) have been identified, the remaining fifteen ~~twenty-five~~ (15 ~~25~~) percent will be based on information received, **should** additional evaluation be necessary, by respondent during a subsequent interview/presentation/site visit of respondent's facilities and services. The committee will forward their recommendations to the Fort Bend County Commissioners Court.

Firms/Respondents shall not contact any members or employees of Fort Bend County regarding this RFP, evaluation, or selection process. See Section 3.0. Contact discovered in any other such manner, is considered grounds for disqualification.

41.0 VENDOR STATUS:

The awarded vendor is required to hold an **active** status on the SAM.gov website, if applicable, <https://sam.gov/content/home>, and with the Texas Comptroller Taxable Entity website <https://mycpa.cpa.state.tx.us/coa/>.

42.0 ATTACHMENTS:

- 42.1 Attachment 1: Medical Plan Participants as of December 2023
- 42.2 Attachment 2: Number of Clinic Appointments
- 42.3 Attachment 3: Clinic Procedure Report

Fort Bend County RFP 25-002

43.0 REQUIRED FORMS:

All respondents submitting are required to complete the attached/included and return with submission:

- 43.1 Vendor Form
- 43.2 W9 Form
- 43.3 Tax Form/Debt/Residence Certification
- 43.4 Proof of Insurance

Participants As Of March 1, 2024

| Active Participants | |
|---------------------|-------|
| Employees | 1,384 |
| Dependents | 2,689 |
| Total Active | 4,073 |

| Retiree Participants | |
|----------------------|-------|
| Retirees | 873 |
| Dependents | 412 |
| Total Retiree | 1,285 |

Number of Clinic Appointments
For Calendar Year 2023

| Quarter | Urgent Care | Primary Care | Occ-Med | Total |
|--------------|-------------|--------------|---------|-------|
| 1 | 1154 | 652 | 110 | 1916 |
| 2 | 890 | 836 | 116 | 1842 |
| 3 | 934 | 796 | 134 | 1864 |
| 4 | 1023 | 784 | 83 | 1890 |
| Annual Total | 4001 | 3068 | 443 | 7512 |

Other Services
For Calendar Year 2023

| | |
|---|------|
| Nurse Visits | 564 |
| Flu Vaccinations | 1200 |
| DOT/Pre-Employment Physicals | 492 |
| Pre-Employment & Post-Accident Drug Testing | 551 |

YTD Procedure Statistics 2023

| Procedure Code | YTD Total |
|--------------------------------|-----------|
| Fort Bend County Clinic | |
| 0591T | 33 |
| | 33 |
| | - |
| 10060 | 3 |
| | 3 |
| | - |
| 10120 | 5 |
| | 5 |
| | - |
| 11200 | 9 |
| | 9 |
| | - |
| 11730 | 2 |
| | 2 |
| | - |
| 11765 | 10 |
| | 10 |
| | - |
| 12001 | 7 |
| | 7 |
| | - |
| 12002 | 1 |
| | 1 |
| | - |
| 12011 | 5 |
| | 5 |
| 12013 | 1 |
| | 1 |
| | - |
| 17000 | 21 |
| | 21 |
| | - |
| 17003 | 1 |
| | 1 |
| | - |
| 20550 | 4 |
| | 4 |
| | - |
| 20551 | 4 |
| | 4 |
| | - |
| 20552 | 1 |
| | 1 |
| | - |
| 20553 | 1 |

| | |
|-------|----|
| | 1 |
| | - |
| 20600 | 1 |
| | 1 |
| | - |
| 20605 | 15 |
| | 15 |
| | - |
| 20610 | 12 |
| | 12 |
| | - |
| 28190 | 1 |
| | 1 |
| | - |
| 29125 | 6 |
| | 6 |
| | - |
| 29505 | 3 |
| | 3 |
| | - |
| 29515 | 1 |
| | 1 |
| | - |
| 36415 | - |
| | - |
| 65205 | 1 |
| | 1 |
| | - |
| 69210 | 6 |
| | 6 |
| | - |
| 70140 | 2 |
| | 2 |
| | - |
| 70160 | 1 |
| | 1 |
| | - |
| 70250 | 2 |
| | 2 |
| | - |
| 71045 | 3 |
| | 3 |
| | - |
| 71046 | 76 |
| | 76 |
| 71100 | 2 |
| | 2 |
| | - |
| 71101 | 7 |
| | 7 |

| | |
|-------|----|
| | - |
| 71110 | 1 |
| | 1 |
| | - |
| 72040 | 23 |
| | 23 |
| | - |
| 72070 | 6 |
| | 6 |
| | - |
| 72072 | 1 |
| | 1 |
| | - |
| 72082 | 2 |
| | 2 |
| | - |
| 72100 | 25 |
| | 25 |
| | - |
| 72110 | 1 |
| | 1 |
| | - |
| 72170 | 3 |
| | 3 |
| | - |
| 72220 | 3 |
| | 3 |
| | - |
| 73000 | 1 |
| | 1 |
| | - |
| 73030 | 42 |
| | 42 |
| | - |
| 73070 | 15 |
| | 15 |
| | - |
| 73090 | 2 |
| | 2 |
| | - |
| 73110 | 27 |
| | 27 |
| | - |
| 73130 | 32 |
| | 32 |
| | - |
| 73140 | 32 |
| | 32 |
| | - |
| 73502 | 27 |

| | |
|-------|-----|
| | 27 |
| | - |
| 73552 | 2 |
| | 2 |
| | - |
| 73560 | 11 |
| | 11 |
| | - |
| 73562 | 63 |
| | 63 |
| 73564 | 1 |
| | 1 |
| | - |
| 73590 | 5 |
| | 5 |
| | - |
| 73610 | 53 |
| | 53 |
| | - |
| 73630 | 57 |
| | 57 |
| | - |
| 73650 | 3 |
| | 3 |
| | - |
| 73660 | 25 |
| | 25 |
| | - |
| 74000 | 14 |
| | 14 |
| | - |
| 74020 | 2 |
| | 2 |
| | - |
| 80061 | - |
| | - |
| | - |
| 80100 | 41 |
| | 41 |
| | - |
| 81000 | 1 |
| | 1 |
| | - |
| 81003 | 328 |
| | 328 |
| | - |
| 81025 | 42 |
| | 42 |
| | - |
| 82075 | 4 |

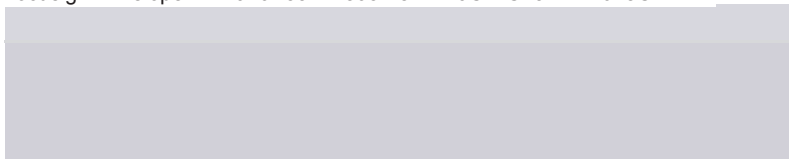
| | |
|--------|-----|
| | 4 |
| 82465 | 9 |
| | 9 |
| | - |
| 82962 | 24 |
| | 24 |
| | - |
| 83036 | 18 |
| | 18 |
| 86308 | 11 |
| | 11 |
| | - |
| 86580 | 12 |
| | 12 |
| 87426 | 784 |
| | 784 |
| 87428 | 11 |
| | 11 |
| | - |
| 87636 | 8 |
| | 8 |
| 87804 | 669 |
| | 669 |
| 87880 | 568 |
| | 568 |
| 90471 | 8 |
| | 8 |
| | - |
| 90630 | 2 |
| | 2 |
| | - |
| 90661 | 1 |
| | 1 |
| | - |
| 90674 | 1 |
| | 1 |
| 90688B | - |
| | - |
| | - |
| 90696A | 1 |
| | 1 |
| | - |

| | |
|--------|-----|
| 90714 | 19 |
| | 19 |
| | - |
| 90714C | - |
| | - |
| 90714D | 5 |
| | 5 |
| | - |
| 90715C | 1 |
| | 1 |
| | - |
| 90746B | 2 |
| | 2 |
| | - |
| 90746C | - |
| | - |
| 90746D | 2 |
| | 2 |
| 90756 | 3 |
| | 3 |
| 93000 | 53 |
| | 53 |
| 96372 | 78 |
| | 78 |
| 99080 | 173 |
| | 173 |
| 99173 | 6 |
| | 6 |
| | - |
| 99202 | 24 |
| | 24 |
| 99203 | 152 |
| | 152 |
| 99204 | 9 |
| | 9 |
| | - |
| 99211 | 74 |
| | 74 |
| 99212 | 101 |
| | 101 |

| | |
|------------|-------|
| 99213 | 4,907 |
| | 4,907 |
| <hr/> | |
| 99214 | 2,000 |
| | 2,000 |
| <hr/> | |
| 99385 | 13 |
| | 13 |
| | - |
| <hr/> | |
| 99386 | 8 |
| | 8 |
| | - |
| <hr/> | |
| 99393 | 1 |
| | 1 |
| | - |
| <hr/> | |
| 99394 | 1 |
| | 1 |
| | - |
| <hr/> | |
| 99395 | 52 |
| | 52 |
| | - |
| <hr/> | |
| 99396 | 155 |
| | 155 |
| | - |
| <hr/> | |
| 99397 | 24 |
| | 24 |
| | - |
| <hr/> | |
| A4565 | 2 |
| | 2 |
| | - |
| <hr/> | |
| CAMPPHY1 | 2 |
| | 2 |
| | - |
| <hr/> | |
| CAMPPHY2 | 3 |
| | 3 |
| | - |
| <hr/> | |
| CUSTSERV | 1 |
| | 1 |
| | - |
| <hr/> | |
| DOTPHY | 94 |
| | 94 |
| | - |
| <hr/> | |
| E0114 | 5 |
| | 5 |
| | - |
| <hr/> | |
| ERTRANS | 10 |
| | 10 |
| | - |
| <hr/> | |
| EXPHYSICAL | 95 |

| | |
|----------|----|
| | 95 |
| | - |
| G0008 | 2 |
| | 2 |
| | - |
| GLOBALFU | 10 |
| | 10 |
| | - |
| J0696 | 17 |
| | 17 |
| | - |
| J1100 | 97 |
| | 97 |
| | - |
| J1200 | 1 |
| | 1 |
| | - |
| J1885 | 24 |
| | 24 |
| | - |
| J2550 | 4 |
| | 4 |
| | - |
| J7512 | 3 |
| | 3 |
| | - |
| J7613 | 1 |
| | 1 |
| | - |
| J7620 | 4 |
| | 4 |
| | - |
| L1820 | 8 |
| | 8 |
| | - |
| L1902 | 9 |
| | 9 |
| | - |
| L3260 | 2 |
| | 2 |
| | - |
| L3809 | 11 |
| | 11 |
| | - |
| L3908 | 12 |
| | 12 |
| | - |
| L4361 | 18 |
| | 18 |
| | - |

| | |
|---|---------------|
| PHYNONDOT | 3 |
| | 3 |
| | - |
| PHYNONDOT1 | 2 |
| | 2 |
| | - |
| PHYNONDOT2 | 196 |
| | 196 |
| | - |
| PHYSICAL | 1 |
| | 1 |
| | - |
| PPVL1 | 11 |
| | 11 |
| | - |
| PPVL2 | |
| | - |
| PREOPEKG | 16 |
| | 16 |
| | - |
| Q4051 | 6 |
| | 6 |
| | - |
| REDRAW | 1 |
| | 1 |
| | - |
| S0119 | 2 |
| | 2 |
| | - |
| S0630 | 3 |
| | 3 |
| | - |
| S9083 | - |
| | - |
| | - |
| SCHPHY1 | 98 |
| | 98 |
| | - |
| TBREAD | 15 |
| | 15 |
| | - |
| VIRTUAL | 2 |
| | 2 |
| | - |
| WKPHYSICAL | 10 |
| | 10 |
| | - |
| Fort Bend County Clinic - Total Counts | 11,933 |



Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

▶ Go to www.irs.gov/FormW9 for instructions and the latest information.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

Occupational Health Centers of the Southwest, P.A.

2 Business name/disregarded entity name, if different from above

Concentra Medical Centers

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

Individual/sole proprietor or single-member LLC C Corporation S Corporation Partnership Trust/estate

Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

PO Box 9005

6 City, state, and ZIP code

Addison, TX 75001

7 List account number(s) here (optional)

Requester's name and address (optional)

Print or type.
See Specific Instructions on page 3.

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

| Social security number | | | | | | | | |
|------------------------|--|--|---|--|--|--|--|--|
| | | | - | | | | | |

or

| Employer identification number | | | | | | | | | |
|--------------------------------|---|---|---|---|---|---|---|---|---|
| 7 | 5 | - | 2 | 0 | 1 | 4 | 8 | 2 | 8 |

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here

Signature of U.S. person ▶

Deanna Chappell

Date ▶

11/1/2024

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)

- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, later.

Note. If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax under section 1446 on any foreign partners' share of effectively connected taxable income from such business. Further, in certain cases where a Form W-9 has not been received, the rules under section 1446 require a partnership to presume that a partner is a foreign person, and pay the section 1446 withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid section 1446 withholding on your share of partnership income.

In the cases below, the following persons must give Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States:

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the entity;
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the trust; and
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust (other than a grantor trust) and not the beneficiaries of the trust.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person, do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Publication 515, Withholding of Tax on Nonresident Aliens and Foreign Entities).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a "saving clause." Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items:

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.
2. The treaty article addressing the income.
3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.
4. The type and amount of income that qualifies for the exemption from tax.
5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if his or her stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first protocol) and is relying on this exception to claim an exemption from tax on his or her scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 28% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester,
2. You do not certify your TIN when required (see the Part II instructions on page 3 for details),

3. The IRS tells the requester that you furnished an incorrect TIN,

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only), or

5. You do not certify to the requester that you are not subject to backup withholding under 4 above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code* on page 3 and the separate Instructions for the Requester of Form W-9 for more information.

Also see *Special rules for partnerships* above.

What is FATCA reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all United States account holders that are specified United States persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code* on page 3 and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you no longer are tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account; for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of \$50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a \$500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account, list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9.

a. **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note. ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040/1040A/1040EZ you filed with your application.

b. **Sole proprietor or single-member LLC.** Enter your individual name as shown on your 1040/1040A/1040EZ on line 1. You may enter your business, trade, or "doing business as" (DBA) name on line 2.

c. **Partnership, LLC that is not a single-member LLC, C Corporation, or S Corporation.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

d. **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. You may enter any business, trade, or DBA name on line 2.

e. **Disregarded entity.** For U.S. federal tax purposes, an entity that is disregarded as an entity separate from its owner is treated as a "disregarded entity." See Regulations section 301.7701-2(c)(2)(iii). Enter the owner's name on line 1. The name of the entity entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2, "Business name/disregarded entity name." If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, you may enter it on line 2.

Line 3

Check the appropriate box in line 3 for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box in line 3.

Limited Liability Company (LLC). If the name on line 1 is an LLC treated as a partnership for U.S. federal tax purposes, check the "Limited Liability Company" box and enter "P" in the space provided. If the LLC has filed Form 8832 or 2553 to be taxed as a corporation, check the "Limited Liability Company" box and in the space provided enter "C" for C corporation or "S" for S corporation. If it is a single-member LLC that is a disregarded entity, do not check the "Limited Liability Company" box; instead check the first box in line 3 "Individual/sole proprietor or single-member LLC."

Line 4, Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space in line 4 any code(s) that may apply to you.

Exempt payee code.

- Generally, individuals (including sole proprietors) are not exempt from backup withholding.
- Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.
- Corporations are not exempt from backup withholding for payments made in settlement of payment card or third party network transactions.
- Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space in line 4.

- 1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2)
- 2—The United States or any of its agencies or instrumentalities
- 3—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities
- 4—A foreign government or any of its political subdivisions, agencies, or instrumentalities
- 5—A corporation
- 6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or possession
- 7—A futures commission merchant registered with the Commodity Futures Trading Commission
- 8—A real estate investment trust
- 9—An entity registered at all times during the tax year under the Investment Company Act of 1940
- 10—A common trust fund operated by a bank under section 584(a)
- 11—A financial institution
- 12—A middleman known in the investment community as a nominee or custodian
- 13—A trust exempt from tax under section 664 or described in section 4947

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

| IF the payment is for . . . | THEN the payment is exempt for . . . |
|--|---|
| Interest and dividend payments | All exempt payees except for 7 |
| Broker transactions | Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012. |
| Barter exchange transactions and patronage dividends | Exempt payees 1 through 4 |
| Payments over \$600 required to be reported and direct sales over \$5,000 ¹ | Generally, exempt payees 1 through 5 ² |
| Payments made in settlement of payment card or third party network transactions | Exempt payees 1 through 4 |

¹ See Form 1099-MISC, Miscellaneous Income, and its instructions.

² However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) written or printed on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37)

B—The United States or any of its agencies or instrumentalities

C—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i)

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i)

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state

G—A real estate investment trust

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940

I—A common trust fund as defined in section 584(a)

J—A bank as defined in section 581

K—A broker

L—A trust exempt from tax under section 664 or described in section 4947(a)(1)

M—A tax exempt trust under a section 403(b) plan or section 457(g) plan

Note. You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have and are not eligible to get an SSN, your TIN is your IRS individual taxpayer identification number (ITIN). Enter it in the social security number box. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN. However, the IRS prefers that you use your SSN.

If you are a single-member LLC that is disregarded as an entity separate from its owner (see *Limited Liability Company (LLC)* on this page), enter the owner's SSN (or EIN, if the owner has one). Do not enter the disregarded entity's EIN. If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note. See the chart on page 4 for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at www.ssa.gov. You may also get this form by calling 1-800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at www.irs.gov/businesses and clicking on Employer Identification Number (EIN) under Starting a Business. You can get Forms W-7 and SS-4 from the IRS by visiting IRS.gov or by calling 1-800-TAX-FORM (1-800-829-3676).

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and write "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, generally you will have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note. Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if items 1, 4, or 5 below indicate otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code* earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

- 1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983.** You must give your correct TIN, but you do not have to sign the certification.
- 2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983.** You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.
- 3. Real estate transactions.** You must sign the certification. You may cross out item 2 of the certification.
- 4. Other payments.** You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).
- 5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions.** You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

| For this type of account: | Give name and SSN of: |
|---|---|
| 1. Individual | The individual |
| 2. Two or more individuals (joint account) | The actual owner of the account or, if combined funds, the first individual on the account ¹ |
| 3. Custodian account of a minor (Uniform Gift to Minors Act) | The minor ² |
| 4. a. The usual revocable savings trust (grantor is also trustee) b. So-called trust account that is not a legal or valid trust under state law | The grantor-trustee ¹ The actual owner ¹ |
| 5. Sole proprietorship or disregarded entity owned by an individual | The owner ³ |
| 6. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A)) | The grantor* |
| For this type of account: | Give name and EIN of: |
| 7. Disregarded entity not owned by an individual | The owner |
| 8. A valid trust, estate, or pension trust | Legal entity ⁴ |
| 9. Corporation or LLC electing corporate status on Form 8832 or Form 2553 | The corporation |
| 10. Association, club, religious, charitable, educational, or other tax-exempt organization | The organization |
| 11. Partnership or multi-member LLC | The partnership |
| 12. A broker or registered nominee | The broker or nominee |
| 13. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments | The public entity |
| 14. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulations section 1.671-4(b)(2)(i)(B)) | The trust |

¹ List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

² Circle the minor's name and furnish the minor's SSN.

³ You must show your individual name and you may also enter your business or DBA name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

⁴ List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see *Special rules for partnerships* on page 2.

*Note. Grantor also must provide a Form W-9 to trustee of trust.

Note. If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records from Identity Theft

Identity theft occurs when someone uses your personal information such as your name, SSN, or other identifying information, without your permission, to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, contact the IRS Identity Theft Hotline at 1-800-908-4490 or submit Form 14039.

For more information, see Publication 4535, Identity Theft Prevention and Victim Assistance.

Victims of identity theft who are experiencing economic harm or a system problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 1-877-777-4778 or TTY/TDD 1-800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to phishing@irs.gov. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484. You can forward suspicious emails to the Federal Trade Commission at: spam@uce.gov or contact them at www.ftc.gov/idtheft or 1-877-IDTHEFT (1-877-438-4338).

Visit IRS.gov to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.

TAX FORM/DEBT/ RESIDENCE CERTIFICATION

(for Advertised Projects)

Taxpayer Identification Number (T.I.N.): 75-2510547

Company Name submitting Bid/Proposal: Concentra Health Services, Inc.

Mailing Address: 5080 Spectrum Drive, Suite 1200W, Addison, TX 75001

Are you registered to do business in the State of Texas? Yes No

If you are an individual, list the names and addresses of any partnership of which you are a general partner or any assumed name(s) under which you operate your business

I. **Property:** List all taxable property in Fort Bend County owned by you or above partnerships as well as any d/b/a names. Include real and personal property as well as mineral interest accounts. (Use a second sheet of paper if necessary.)

| <u>Fort Bend County Tax Acct. No.*</u> | <u>Property address or location**</u> |
|--|---------------------------------------|
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |

* This is the property account identification number assigned by the Fort Bend County Appraisal District.
 ** For real property, specify the property address or legal description. For business personal property, specify the address where the property is located. For example, office equipment will normally be at your office, but inventory may be stored at a warehouse or other location.

II. **Fort Bend County Debt** - Do you owe any debts to Fort Bend County (taxes on properties listed in I above, tickets, fines, tolls, court judgments, etc.)?

Yes No If yes, attach a separate page explaining the debt.

III. **Residence Certification** - Pursuant to Texas Government Code §2252.001 *et seq.*, as amended, Fort Bend County requests Residence Certification. §2252.001 *et seq.* of the Government Code provides some restrictions on the awarding of governmental contracts; pertinent provisions of §2252.001 are stated below:

- (3) "Nonresident bidder" refers to a person who is not a resident.
- (4) "Resident bidder" refers to a person whose principal place of business is in this state, including a contractor whose ultimate parent company or majority owner has its principal place of business in this state.

I certify that Concentra Health Services, Inc. is a Resident Bidder of Texas as defined in Government Code §2252.001.
[Company Name]

I certify that _____ is a Nonresident Bidder as defined in Government Code §2252.001 and our principal place of business is _____.
[Company Name] [City and State]

EXHIBIT D:
Performance Indicators/Objectives

| Category | Performance Guarantee | Onsite Model Application | Definition | Program Requirements | Measurement and Performance |
|-------------|--|--|--|--|--|
| Operational | Wait Time | Occupational and Urgent / Primary Care | Average wait time in the onsite clinic is defined as the time from the patient sign in to check-in. | Concentra's EMR must be deployed | <15 minute wait time |
| Operational | Missed Appointment Percent | Occupational and Urgent / Primary / Preventive | Measures the percent of missed scheduled appointments | Concentra's EMR must be deployed | <10% of visits would have missed appointments and not be rescheduled |
| Operational | Patient Net Promoter Score (NPS) | Occupational and Urgent / Primary / Preventive | NPS is on a scale of -100 to 100 and equals the (% Promoters score of 9-10) – (% Detractors score 0-6) from the question from Patient Satisfaction Survey: How likely would you be to recommend this worksite to your co-workers? Scale: Promoters – 9-10; Passives – 7-8; Detractors – 0-6. Measure - % of promoters-% of detractors. | Client must have satisfaction surveys administered by Concentra (vs. by the client) | NPS score - >85% |
| Clinical | Adult Health Data Collection and Reporting | Urgent / Primary / Preventive | Biometric screening will be collected annually for all adult patients treated at the clinic along with verifications of a history of tobacco use. | Concentra's EMR must be deployed for reporting results Client must have biometric screening program requirement | |
| Operational | Facility Audits | Occupational and Urgent / Primary / Preventive | An onsite facility audit will be performed by operations 2x/year using our Compliance Audit Tool (CAT). The results will be shared with client and any corrective action plan will be prioritized and enacted within 30 days or in a mutually determined reasonable timeframe. | Audit results and deficiencies must be reported to the client. | 100% CAT score |

EXHIBIT E:
COUNTY TRAVEL POLICY

Annex B

Fort Bend County Travel Policy

Approved in Commissioners' Court on November 3, 2009

Effective November 4, 2009

Revised September 7, 2010

Revised June 2, 2015, Effective August 1, 2015

Revised July 28, 2015, Effective August 1, 2015

Revised July 26, 2016, Effective August 1, 2016

Revised December 12, 2017, Effective January 1, 2018

Revised September 26, 2023, Effective October 1, 2023

The Commissioners' Court allocates funds annually for the payment of travel expenditures for county employees and officials within the individual departmental budgets. Travel expenditures paid from these budgets must serve a public purpose for Fort Bend County. These expenditures may be paid directly to the vendor or provided as a reimbursement to the employee/official upon completion of their travel. Advance payments to vendors may be accommodated by issuance of a check or use of a County procurement card. Eligible expenditure categories under this policy include: Lodging, meals, transportation, registration fees, and other fees (with justification). Each category is further defined below.

CONTRACT RATES:

Fort Bend County is a 'Cooperative Purchasing Participating Entity' with the State of Texas. This program is also known as TPASS (Texas Procurement and Support Services) State Travel Management Program (STMP). This gives County employees and officials access to the contract rates negotiated by the State for hotels and rental cars. Procurement procedures for these contract services are explained within the categories below.

OUT OF STATE TRAVEL:

Authorization: The traveler must obtain Commissioners' Court approval for out-of-state travel before departure. The duration must include travel days along with the event scheduled days. To prevent delays in processing travel reimbursement, ensure that the travel duration is accurately defined when submitting the agenda request.

Documentation: The traveler must provide an excerpt from the Commissioners' Court minutes (<http://www.fortbendcountytexas.gov/index.aspx?page=55>) with the travel reimbursement form.

LODGING (In and Out of State):

Hotel:

Hotel reimbursements are limited to the Federal Travel Regulations set forth by US General Services Administration (GSA) by location not including taxes. The rates are set annually and vary by month and location. The maximum rates for lodging per day can be found at:

http://www.gsa.gov/portal/content/104877?utm_source=OGP&utm_medium=print-radio&utm_term=perdiem&utm_campaign=shortcuts based on travelers destination.

Fort Bend County is a 'Cooperative Purchasing Participating Entity' with the State of Texas. This gives County employees and officials access to the contract rates negotiated by the State for hotels. Participating hotels can be found at: https://portal.cpa.state.tx.us/hotel/hotel_directory/index.cfm (be sure to check the correct fiscal year). **When making a reservation the traveler must ask for the State of Texas**

Contract rate (not the government rate) and be prepared to provide the County's agency #: C0790. Traveler must verify confirmed rate matches the negotiated contract rates found on the State's website listed above and does not exceed the GSA daily allowance.

If the organizer of a conference/seminar has negotiated discount rates with a hotel(s), the traveler may choose these lodging services without penalty but the traveler must reserve the room at the group rate and provide documentation of the group rate with the reimbursement request.

If all rooms are booked at the host hotel and no accommodation is available at or below the GSA rate, you may book a room at another hotel at a rate equal to or lower than the conference/seminar rate.

If all rooms are booked at the host hotel and no accommodation is available at or below the GSA rate or at the conference/seminar rate, you may provide three (3) comps to support the higher rate. This will serve as the justification for the higher rate. The comparable hotels should be within five miles of the host event and should be of similar hotel class.

The traveler will be responsible for the excess charge over the GSA per diem rate for the city/county even if using the State rate. The Auditor's Office will deduct from the travelers' reimbursement any excess charges over the GSA per diem rate.

If a traveler cannot find a traditional hotel, a direct rental (Airbnb, VRBO, etc.) is allowable. All previous maximum daily rates still apply. Any fees incurred through a direct rental must also be included in the daily rate calculation and remain below the limits. Fees may include, but are not limited to, cleaning fees, extra guest fees, or service fees. (Taxes are not included in this calculation, as they are charged to hotel stays as well).

Travel websites including but not limited to Expedia and Travelocity shall not be used to book lodging.

In order to qualify for any of the above-mentioned exceptions, a lodging reservation must be made 14 days prior to travel. If travel is required without 14-day notice, the traveler must provide back-up which explains why the 14-day advance booking was not possible.

Travel Days: If the traveler must leave before 7:00AM to arrive at the start of the event and/or return to the County after 6:00PM after the event concludes, an additional night's lodging is allowable before and/or after the event.

Additional fees allowable: Self-parking

Additional fees allowable with justification: Valet parking is allowable if an extreme hardship exists due to physical disability of the traveler or if no self-parking is available.

Fees not allowable: Internet, phone charges, laundry, safe fees

Gratuities: Gratuities are not reimbursable for any lodging services.

Overpayments by County: Any lodging overpayment by the County must be reimbursed by the hotel before processing a reimbursement to the traveler for any of the categories addressed in this policy. Prepaid lodging services should be accurately calculated or underestimated by excluding the taxes to prevent delays in processing travel reimbursements.

Procurement Card: The traveler may use the procurement card to make lodging reservations. Contact Purchasing to arrange or use the procurement card assigned to the department or traveler.

Documentation: A final settled hotel bill with a zero balance from the front desk is required even if lodging is paid by the procurement card. The hotel bill left under the door is not acceptable. The hotel bill should be scrutinized before traveler departs to make sure all charges are valid and notify hotel of any invalid charges and resolve issues before departing. Make sure all parking has been added to your bill and all personal incidentals have been paid by traveler. Any invalid charges will be the responsibility of the traveler. A copy of the itemized hotel statement must be submitted with the travel reimbursement claim if the traveler used a County procurement card to purchase lodging services or prepaid by County check. Event agenda/documentation or a letter from the traveler describing the event/meeting is required. If utilizing conference negotiated hotel rates, documentation of rates is required.

Changes/Modifications to Reservation – Any modifications including cancellation of reservation, the traveler must obtain a confirmation number and note the name of the person they spoke with in case the hotel charges the traveler. If the traveler does not obtain a confirmation number then any expenses incurred will be the responsibility of the traveler. Expenses resulting from changes or modifications to travel reservations will be paid by the County if the traveler produces documentation that a family emergency exists.

County Exemption Status – Fort Bend County Employees traveling on County Business are not exempt from State and local hotel taxes, state taxes, etc. with the exception of District Judges and the District Attorney.

MEALS:

Meals including in-state and out-of-state will be reimbursed to the traveler at a flat rate of \$70 (full day). The travelers per diem on the departure day and final day will be at 75% of the per diem, which is \$52.50. The amount reimbursed will be paid through payroll and is subject to federal taxation.

Late Night Arrival – If a traveler arrives in Fort Bend County between midnight and 6am the traveler will receive a full day per diem for the previous day.

Day trips: Prior to 01/01/2024 – Meals will not be reimbursed for trips that do not require an overnight stay. Effective 01/01/2024 - The traveler is subject to per diem reimbursement. Day trip includes a trip outside the County that requires a traveler to leave Fort Bend before 7:00 AM and/or return to the County after 6:00 PM will be eligible for reimbursement at 75% of the per diem, which is \$52.50. Amount reimbursed for day trips will be paid through payroll and are subject to federal taxation.

Procurement Card: No meal purchases are allowed on any County procurement card.

Documentation: No meal receipts are required for reimbursement. Event agenda/documentation or a letter from the traveler describing the event/meeting is required.

TRANSPORTATION:

Personal Vehicle: Use of personal vehicle will be reimbursed at the current rate/mile set by Commissioners' Court. Mileage should be calculated using the County office location of the traveler and the event location. Mileage may not be calculated using the traveler's home. Mileage should be calculated using an employees vehicle odometer reading or by

a readily available online mapping service for travel out of Fort Bend County. If using the mileage of an online mapping service, state which mapping service was used or provide a printout of your route detailing the mileage. For local travel, odometer readings or mapping service details are not required. Departments should develop a mileage guide for employees for local travel points, if a department does not have a mileage guide, the Auditor's Office will determine if the mileage listed is reasonable.

Allowable expenses: Parking and tolls with documentation.

County Vehicle: Fuel purchases when using a County vehicle should be made with the County Procurement card if available. Original receipts will accompany the Procurement Card statement but a copy must be provided with the travel reimbursement request.

Allowable expenses: Parking and tolls with documentation required.

Airfare: The County will only reimburse direct travel to and from a location where County-related business is being conducted. Airfare is reimbursable at the lowest available rate based on 14 day advance purchase of a discounted coach/economy full-service seat based on the required arrival time for the event. The payment confirmation and itinerary must be presented with the travel reimbursement form. The traveler will be responsible for the excess charges of an airline ticket purchase other than a coach/economy seat. When using Southwest Airlines a traveler should choose the "wanna get away" flight category.

Allowable Expenses: Bag fees. Fare changes are allowable if business related or due to family emergency.

Unallowable Expenses/Fees: Trip insurance, Early Bird Check In, Front of the line, Leg Room, Fare changes for personal reasons.

Rental Car: Rental cars are limited to the negotiated TPASS rates listed at: <http://www.window.state.tx.us/procurement/prog/stmp/stmp-rental-car-contract/vendor-comparison/>. The contact information for Enterprise for the State Travel Management Program is listed here: <https://comptroller.texas.gov/purchasing/programs/travel-management/rental/enterprise.php>

When making a reservation traveler should provide the County's agency # [REDACTED]. The traveler will not be reimbursed for any amount over the negotiated contract rates if a non-contract company is used at a higher rate. The traveler should select a vehicle size comparable to the number of County travelers. The traveler may use a non-contract vendor at an overall rate lower than the contract rates with no penalty. The original contract/receipt must be presented with the travel reimbursement form or a copy if a County procurement card is used. . The traveler will be responsible for any excess charges not included in the TPASS rates or for choosing a vehicle size not comparable with the number of travelers on the trip. Insurance is included in the negotiated TPASS rates, if a traveler chooses to take out additional insurance the cost is on the traveler.

Enterprise:

- Optional Customer, Coupon or Corporate number is [REDACTED]
- [REDACTED]
- Enterprise will automatically bill FBC when you reserve your vehicle so you need to have a purchase order before your departure.

Unallowable Fees/Charges: GPS, prepaid fuel, premium radio, child safety seats, additional insurance, one way rentals.

Allowable expenses: Parking and tolls allowed with documentation.

Other Transportation: Other forms of transit (bus, taxi, train) are reimbursable with an original receipt.

Gratuities: Gratuities are permitted if original receipt includes gratuity (20% maximum allowed) for any transportation services.

Procurement Card: The traveler may use a County procurement card to make transportation reservations for air travel and rental car services. Contact Purchasing to arrange or use the procurement card assigned to the department or traveler.

Documentation: Original receipts are required for all transportation reimbursements paid by the traveler. Transportation services obtained with a County procurement card require a copy of the receipt. Additional requirements are noted within each category above. Event agenda/documentation or a letter from the traveler describing the event/meeting is required.

REGISTRATION:

Registration fees: Registration fees are reimbursable for events that serve a Fort Bend County purpose. Registration fees for golf tournaments, tours, guest fees and other recreational events are not reimbursable.

Procurement Card: The traveler may use a County procurement card to register for an event. Contact Purchasing to arrange or use the procurement card assigned to the department or traveler.

Documentation: An original receipt must be obtained upon registration and submitted with the reimbursement request if paid by the traveler. A copy of the receipt must be provided if registration is paid on a County procurement card. Event agenda/documentation or a letter from the traveler describing the event/meeting is required.

GRANTS:

Travel expenditures from Federal and State grants must also conform to the granting agency's funding requirements.

TRAVEL REIMBURSEMENT FORM:

The traveler must use the current travel reimbursement form <https://econnect.fortbendcountytx.gov/documents-forms/auditors-office-forms> for all travel related services addressed in this policy. No other expenditures may be submitted for reimbursement on the travel reimbursement form. After completing all required information, the travel form must be signed/dated by the traveler and the department head/elected official. Travel reimbursement request should be submitted within 30 days from when traveler returns from trip. Mileage reimbursement request should be submitted no less frequently than quarterly. Mileage reimbursement request for the fourth quarter should be submitted no later than October 30th for yearend processing.

EXCLUSIONS:

If the traveler has custody of a person pursuant to statute or court order or if the traveler is required by court or legal entity to appear at a particular time and place the traveler will not be penalized for accommodations that require a 14 day advance purchase ticket if travel is required with less than 14 days' notice.

If the traveler has custody of a person pursuant to statute to court order the traveler will not be held to the 75% per diem on the departure and final day of travel.

EXHIBIT F:
SECURITY REQUIREMENTS



Training and Education

| | |
|--------------|--------------------------------|
| Number | H02-A |
| Policy Owner | Privacy Officer |
| Approved By | Privacy and Security Committee |

| | |
|--------------------|------------|
| Effective Date | 4/14/2003 |
| Last Revision Date | 10/16/2020 |
| Page | 1 of 2 |

PURPOSE

Select Medical Corporation (Select Medical) is obligated under the federal HIPAA privacy regulations to train all members of its workforce on the policies and procedures required by the federal regulations with respect to the privacy of patient health and medical information. The Privacy Officer and his/her designees are charged with developing training schedules and programs so that all workforce members receive the necessary training that is appropriate to permit the workforce members to carry out their functions within Select Medical.

POLICY

It is the policy of Select Medical that all members of its workforce are trained and educated with respect to the privacy of patient health and medical information as identified under the Federal Health Insurance Portability and Accountability Act (HIPAA), including the Privacy Rule, Security Rule, and Breach Notification Rule.

PROCEDURES

- General Training.** All members of the workforce are required to receive general training to cover topics in the Privacy Rule, Security Rule, and Breach Notification Rule.

Topics to be covered will include:

- The responsibilities of all members of the workforce with respect to patients' health and medical information as set forth in Policy "H03-A Workforce Obligations";
- The privacy policies and procedures of Select Medical which are applicable to all members of the workforce;
- The personal and ethical obligations of each individual with respect to patients' health and medical information; and
- The disciplinary actions and legal sanctions are applicable to individuals who violate the privacy policies and procedures.

- Security Training.** All members of the workforce are required to receive HIPAA security training to cover topics in the Security Rule and information security awareness requirements.

Topics to be covered will include:

- Raise and maintain awareness of security issues;

- The security policies and procedures of Select Medical which are applicable to all members of the workforce;
 - Awareness with regard to protection from malicious software, including procedures for guarding against, detecting and reporting malicious software; such as, viruses and worms;
 - Familiarity with procedures for monitoring log-in attempts and reporting discrepancies;
 - Awareness with regard to procedures for creating, changing and safeguarding passwords.
3. **Training Format.** The Privacy Officer will design a format for the general training and education program which is most effective for communication to the existing workforce members. The program may include live presentations, video presentations, written handouts, web-based training, or other effective means of training.
 4. **New Workforce Member Training.** All newly hired workforce members will receive general and security HIPAA training within thirty days (30) of being hired.
 5. **Annual Training.** All workforce members will receive general and security HIPAA training annually.
 6. **Records and Documentation.** The Privacy Officer shall assure that records of training and education are maintained.
 7. **Additional Communications.** Periodic Communications will be provided through a variety of other means, including orientation, written materials, newsletters, broadcast e-mails, staff meetings and formal internal and external education. These communications will provide HIPAA and Security reminders and updates.

Policy References:

H03-A Workforce Obligations



Workforce Obligations

| | |
|--------------|--------------------------------|
| Number | H03-A |
| Policy Owner | Privacy Officer |
| Approved By | Privacy and Security Committee |

| | |
|--------------------|-----------|
| Effective Date | 4/14/2003 |
| Last Revision Date | 1/27/2021 |
| Page | 1 of 5 |

PURPOSE

Select Medical Corporation (Select Medical) collects and maintains certain PHI about our patients. In order to protect the privacy and confidentiality of our patients' PHI and to comply with federal law, all members of the workforce of Select Medical are required to comply with the provisions of this policy.

POLICY

It is the policy of Select Medical that all members of its workforce must comply with this policy regarding the use and disclosure of a patient's protected health information (PHI) as a condition of their employment or continued relationship with Select Medical.

PROCEDURES

1. PHI of a patient may not be used for any purpose other than:
 - a) For treatment, payment, or health care operations and purposes consistent with Policy "H01-A Uses and Disclosures of Protected Health Information (PHI)" policy and procedure;
 - b) As required by the individual's job description or employment duties, unless such use is specifically authorized by a signed authorization from the patient;
 - c) As specified by a Select Medical policy and procedure;
 - d) Has been approved by the Privacy Officer.

2. When disclosing a patient's PHI, all reasonable efforts must be made to limit the information used or disclosed to that, which is minimally necessary to accomplish the purpose of the use or disclosure. This requirement does not apply to the following uses and disclosures of the information:
 - Disclosures to or requests by a health care provider for treatment purposes;
 - Disclosures to the patient whose information is the subject of the disclosure;
 - Disclosures to the U.S. Department of Health and Human Services for compliance and investigation purposes; and
 - Uses or disclosures required to be made by law.

3. All workforce members must complete general education and security HIPAA training within 30 days of being hired and on an annual basis. All workforce members are required to understand and adhere to the standards and policies of Select Medical, which relate to the use and disclosure of personal health information; and seek guidance and training when necessary to resolve questions about the standards and policies.

4. According to Policy “H06-A Disclosures to Individuals Involved with Patient’s Care”, it is Select Medical’s practice to obtain approval from the patient prior to sharing PHI with persons involved with the patient. When the patient is unavailable or unable to agree due to incapacity or emergency, such disclosure may be made if it is deemed in the best interest of the patient. The Privacy Officer should be contacted in the event that there are any questions in making the determination. It is common for patients to have individuals, such as family members and/or people involved in some aspect of caring for them or paying for their care. In such situations it may be beneficial to share PHI regarding the patient with the individual involved in the patient’s care to facilitate his or her involvement with the care of the patient or payment for such care.

5. Patient information may not be used for internal research or disclosed to anyone outside Select Medical for research without specific approval from the Privacy Officer or the Research Committee. Reference “Disclosures for Research Purposes” Policy.

6. Patients of Select Medical have certain rights required by HIPAA. In order to assure that these rights are not compromised, all workforce members must be aware of these rights and the following duties and responsibilities:
 - a) **Access to PHI.** A patient has the right to inspect and obtain a copy of any PHI which we may possess concerning the patient. Patients also have a right to obtain an electronic copy of PHI that is maintained in any electronic system. Any such request made by a patient or their personal representative may be made in oral or in written form and submitted to Select Medical. The requestor may use the Patient Access Form in Policy H08-B, if they so choose. If the individual makes the request in oral form, then the individual fulfilling the request should complete the Access Form and indicate “Verbal Request” at the top of the form. If the request is for an electronic copy of PHI, we must provide the individual with access to the PHI in the electronic form and format requested by the individual if it is readily producible in such a form and format, or, if not, in a readable electronic form as agreed to by us and the patient. Requests shall be responded to within 30 days in accordance with the requirements of § 164.524(b).
 - b) **Amendments to PHI.** Patients have the right to request that Select Medical make amendments to their PHI. If a patient or the patient’s legal representative requests an amendment to his/her PHI, the patient or patient’s legal representative must complete the “Amendment of Medical Record Form”(refer to Policy “H12-A Right to An Amendment”). The “Amendment of Medical Record Form” can be obtained from the individual responsible for medical records. If you receive an “Amendment of Medical Record Form”, the form must be promptly forwarded to the individual responsible for medical records.
 - c) **Accounting for Disclosures.** Patients have the right to request that Select Medical provide an accounting to them of disclosures that have been made for purposes other than treatment, payment and health care operations, purposes required by law or pursuant to a valid authorization. If a patient or the patient’s legal representative requests such an accounting, the patient or the patient’s legal representative must complete the “Accounting Request Form” (refer to Policy “H15-

A Processing Requests for an Accounting of Disclosures of Protected Health Information”). The “Accounting Request Form” can be obtained from the individual responsible for medical records. If you receive an “Accounting Request Form”, the form must be promptly forwarded to the individual responsible for medical records. **Restrictions:** Patients have the right to request a restriction on the uses and disclosures of his/her PHI. Once the request has been approved in accordance with Policy “H11-A Patient Requests for Restriction”, then the PHI may not be used or disclosed for any purpose in violation of such restriction, except as necessary for the emergency treatment of the patient. Before using or disclosing any PHI, it is the responsibility of the individual responsible for medical records to determine whether any restriction exists and to act consistent with the restriction.

- d) **Confidential Communications:** Patients have the right to request to receive communications from us by alternative means or at alternative locations. For example, patients may ask us to only send appointment reminder cards in sealed envelopes rather than on postcards, or to call them only at work rather than at home. All reasonable requests will be accommodated consistent with Policy “H13-A Confidential Communications”. Before communicating with any patient, determine whether a confidential communication restriction exists.
 - e) **Complaints.** Patients have the right to file a complaint with Select Medical if they believe that their privacy rights have been violated. If any person requests information on how to file a complaint, you may give them the address of Select Medical’s Privacy Officer at 4714 Gettysburg Road, P.O. Box 2034, Mechanicsburg, PA 17055. Patients also have the right to file complaints with the Secretary of the U.S. Department of Health and Human Services.
 - f) **No Waiver of Rights.** No member of the workforce can require a patient to waive any of the rights set forth in this policy as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
7. **Verification of Identity.** It is the policy of Select Medical to verify the identity of a person requesting PHI and the authority of any such person to have access to that PHI, if the identity or authority of such person is not known (refer to Policy “H10-A Verification of Identity and Authorization” policy for further detail and information).
8. **Privacy and/or Security Violations.** All workforce members must promptly notify the Privacy Officer if they become aware of any misuses of a patient’s PHI. Workforce members should also work with the Privacy Officer to mitigate any harmful effect that is known regarding the uses or disclosure of PHI in violation of this or other policy of Select Medical.
9. **Business Associates.** Select Medical has agreements with Business Associates who use PHI in the provision of services to and on behalf of Select Medical. These agreements include provisions that require the Business Associate to keep our patients’ PHI confidential. If an employee has any information regarding a possible privacy violation by a Business Associate, such information must be reported to the Privacy Officer within three business days of obtaining such information. Refer to Policy “H16-A Business Associates.”

- 10. Safeguarding Protected Health Information.** All workforce members must take reasonable steps to safeguard personal health information from any intentional or unintentional use or disclosure that is in violation of this or any other policy of Select Medical. Such safeguarding includes, but is not limited to, storing personal health information in a cabinet or closed file at the end of the workday; maintaining privacy during verbal discussions of personal health information; restricting electronic transmission of personal health information to job related duties; and disposing of documents in accordance with policies of Select Medical. Refer to Policy “H04-A Safeguarding Protected Health Information.”
- 11. Non-Retribution Policy.** It is the policy of Select Medical that no employee will be intimidated, threatened, coerced, discriminated against, or have any other retaliatory action taken against them, including workforce members, patients, visitors, and others for the exercise of any right set forth in this policy, including the filing of a complaint to Select Medical or to the Secretary of the U.S. Department of Health and Human Services; for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing regarding the federal law on patient privacy; or for opposing any act or practice made unlawful by the federal patient privacy law or privacy policies of Select Medical, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of personal health information in violation of federal law or a policy of Select Medical. Refer to Policy “H17-A Non-Retribution.”
- 12. Compliance Investigations and Reviews.** Federal law authorizes the Secretary of the U.S. Department of Health and Human Services or a designee to conduct compliance investigations of and reviews to Select Medical’s compliance with the federal HIPAA regulations. We are required to cooperate with such an investigation or review and if you receive a telephone call or visit regarding such an investigation or review you must immediately contact Select Medical’s Legal Department or Compliance Department.
- 13. Marketing Program and Activities.** It is the policy of Select Medical that an authorization (Refer to Policy “H08-A Patient Authorization”) from the individual must be obtained prior to sending them any marketing materials about Select Medical and/or the services that we provide unless the marketing falls within an exception identified by the Health Insurance Portability and Accountability Act (HIPAA).
- 14. Affiliated Covered Entity.** As an Affiliated Covered Entity, Select Medical and its subsidiaries will develop and implement the policies, procedures and protocols as required by the HIPAA regulations. Designation as an ACE will further Select Medical’s goal of quality patient care by allowing for the use and disclosure of PHI, in accordance with the HIPAA regulations, among Select Medical’s clinical and business functions. Refer to Policy “H19-A Designation as Organized Health Care Arrangement for Purposes of HIPAA Compliance.”
- 15. Noncompliance Sanctions and Disciplinary Action.** It is the policy of Select Medical that disciplinary action relating to violations of policies and procedures concerning the privacy of

patient information will be taken in a timely manner to eliminate unacceptable conduct and enforce compliance with the HIPAA privacy regulations. The disciplinary measures taken will be consistent with the violation and the circumstances of each case. Discipline for such infractions of our privacy policies and procedures may include reprimand, suspension, or discharge of the responsible workforce member, depending on the severity of the misconduct. Refer to Policy “H35-A Disciplinary Procedures.”

16. **Psychotherapy Notes.** It is the policy of Select Medical that in those instances psychotherapy information becomes a part of the medical record, a patient authorization must be obtained from the patient or the patient’s legal representative prior to using or disclosing psychotherapy information unless an exception applies. Refer to the appropriate access and authorization policies.

Policy References:

H01-A Uses and Disclosures of Protected Health Information (PHI)
H04-A Safeguarding Protected Health Information
H06-A Disclosures to Individuals Involved with Patient’s Care
H08-B Patient Access to Protected Health Information
H10-A Verification of Identity and Authorization
H11-A Patient Requests for Restriction
H12-A Right to an Amendment
H13-A Confidential Communications
H15-A Processing Requests for an Accounting of Disclosures of Protected Health Information
H16-A Business Associates
H17-A Non-Retribution
H19-A Designation as Organized Health Care Arrangement for Purposes of HIPAA Compliance
H35-A Disciplinary Procedures



Remote Access to Company Network

| | |
|--------------|--------------------------------|
| Number | H37-A |
| Policy Owner | Privacy Officer |
| Approved By | Privacy and Security Committee |

| | |
|--------------------|-----------|
| Effective Date | 4/14/2003 |
| Last Revision Date | 1/29/2024 |
| Page | 1 of 2 |

PURPOSE

Select Medical Corporation (Select Medical) provides workforce members the ability to remotely connect to the Select Medical network, where necessary to fulfill job duties.

To establish guidelines for remote connections to the Select Medical network that include, but are not limited to network connections via dial-up; IPSec VPN over a dial-up, cable, DSL, wireless broadband or satellite broadband connection; or a web browser SSL connection, i.e. MySelect.

POLICY

It is the policy of Select Medical that workforce members who wish to connect to the Select Medical network through a remote access connection must adhere to the procedures and guidelines in this policy. Remote access is a privilege and will be provided only if business justification warrants the access. All workforce members must adhere to the guidelines set forth below and in the IT101 - Information Security Policy.

PROCEDURES

Standards

1. Any workforce member requiring remote access must route that request to the Information Services Department via IT201 – UAR Procedure.
2. Any workforce member requesting remote access while traveling internationally must follow IT208 – System Access for International Travel Procedure.
3. If remote access to Select Medical’s internal network resources is granted, the workforce member must maintain a work environment that meets security and confidentiality requirements for interacting with sensitive data as defined by Select Medical’s policies and procedures as well as established law.
4. Only a Select Medical workstation that is issued to the workforce member by the Information Services Department is authorized to connect to Select Medical’s network.
5. If only limited access to an application(s) or functionality is required, remote access may be provided through a web browser SSL connection to authorized workforce members rather than providing a Select Medical workstation.
6. Where possible, the Select Medical workstation must have an approved firewall installed and active at all times.

7. All remote access should require the workforce member to enter a user ID, password and where feasible, two-factor authentication to gain access and should not make use of any type of feature that would bypass this requirement unless a feature is specifically approved by the Chief Information Officer or Chief Information Security Officer.
8. Workforce members should always be aware of their surroundings in public or private places when accessing ePHI or sensitive information. The workstation should be safeguarded so that information cannot be accessed, viewed and/or heard by any unauthorized individuals.
9. Workforce members should never leave a remote connection unattended. If you must leave the workstation, secure the session by logging off and closing all open connections and windows or lock the workstation so that it requires authentication to gain access again.
10. The technology described within this policy and the desire to work remotely is not business justification for a Select Medical workstation.
11. Remote connections to the Select Medical network are for business purposes only. Select Medical reserves the right to monitor or report on all activity or usage without notification to the workforce member and may revoke remote access privileges at any time in its sole discretion.
12. Manager must notify Select Medical Information Services no later than the day of separation to disable all company access via a termination user access request or direct communication.

Support

1. Workforce member should follow basic troubleshooting steps to confirm that they have active Internet connection with their service provider before contacting the Select Medical Help Desk.
2. Select Medical will not provide technical support for any personal home network or equipment including but not limited to computers, routers, switches, peripherals, or software.
3. Select Medical will not be responsible for the loss, damage, failure or destruction of workforce member-owned computer equipment including, but not limited to computers, routers, switches, peripherals, or software while in use for company or personal business.

Reimbursement

1. Select Medical will not reimburse a workforce member for fees associated with dial-up, cable, DSL, wireless broadband or satellite broadband connections or access from a hotel, airport or coffee shops. See Business and Travel Expenses Policy for clarification.

2. Select Medical will not reimburse a workforce member for any additional equipment or software needed or required by Select for the workforce member to connect from home.

Policy References:

IT101 - Information Security Policy

Business and Travel Expense Policy

IT201 – UAR Procedure

IT208 – System Access for International Travel Procedure



Breach Notification

| | |
|--------------|--------------------------------|
| Number | H39-A |
| Policy Owner | Privacy Officer |
| Approved By | Privacy and Security Committee |

| | |
|--------------------|-----------|
| Effective Date | 4/14/2003 |
| Last Revision Date | 1/23/2018 |
| Page | 1 of 4 |

PURPOSE

This policy sets forth the framework for Select Medical Corporation’s (Select Medical) compliance with Breach Notification provisions within the HIPAA Breach Notification Rule.

POLICY

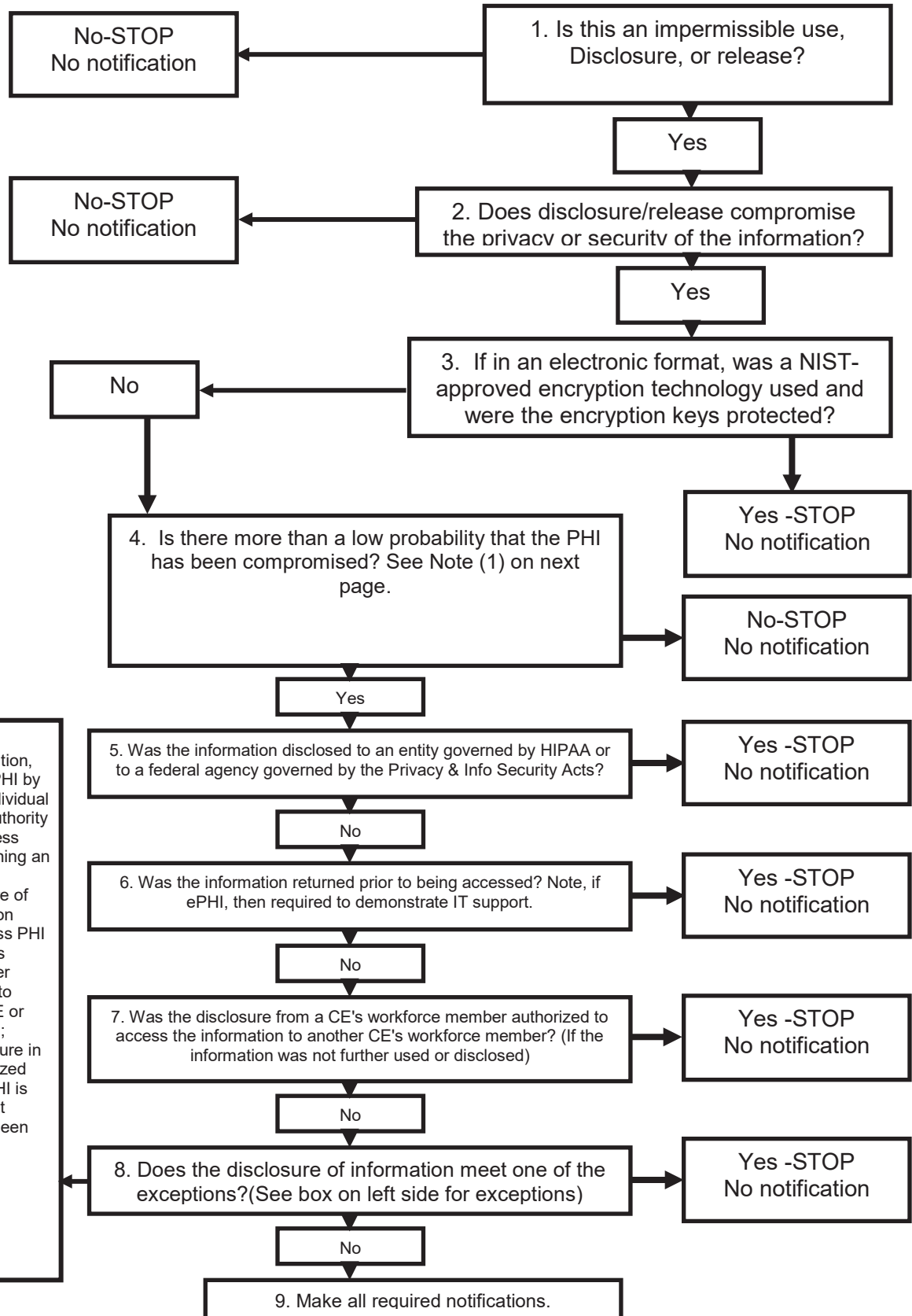
It is the policy of Select Medical that all employees will access, use, and disclose protected health information (PHI) only as permitted under the HIPAA Privacy Rule and, as amended by the HITECH Act. Further, all employees shall be vigilant with respect to guarding PHI. In the event that a breach of unsecured PHI occurs, the following procedures will be followed.

PROCEDURES

- 1) **Use and Disclosure** – All Select Medical employees or individuals acting under the authority of Select Medical or Business Associate must adhere to the Policy and Procedures outlined in “H01-A: Uses and Disclosures of Protected Health Information (PHI).”
- 2) **Reporting a Breach** – Any workforce member, business associate, or data owner who believes that a breach has occurred, should immediately notify their Supervisor(s) and/or a Select Medical representative of the occurrence. The potential breach should then be reported to the Privacy Officer. This can be done directly via phone or e-mail to the Privacy Officer, through the HIPAA Help Line at 717-730-4230, by email at HIPAAHelp@selectmedical.com or through any other Select Medical Compliance Program reporting mechanism. For Concentra locations, notify the Concentra Privacy Office at 800-819-5571 or e-mail: privacyoffice@concentra.com.
- 3) **Breach Notification Risk Assessment** – The Privacy Officer will determine whether the incident is a Security Incident, Breach, or both. The Privacy Officer will work together with the IT Security Team in response to all Security Breaches. The Breach Notification Risk Assessment Tool (Attachment A) will be utilized to determine the appropriate breach notification requirements. For Concentra locations, submit a HIPAA incident report, and the Concentra Privacy Office will work with staff to appropriately mitigate the HIPAA incident.
- 4) **Breach Notification** – In the event the Breach Notification Risk Assessment determines a requirement to notify the affected individuals, HHS, and others, the Privacy Officer will designate an appropriate Company representative to proceed with the required notifications following the procedures in Breach Notification Process (Attachment B).
- 5) **Disciplinary Action** - If a Breach is determined to be the result of workforce member negligence, action, or inaction, the Privacy Officer will work together with Human Resources to consult the workforce member and determine if any further action is required in accordance with the policy H35-A - Disciplinary Procedures.
- 6) **Internal Reporting** - Once this process concludes, the Privacy Officer will report the incident, findings, and actions to the HIPAA Committee at the next meeting.

Attachment A

Breach Notification Risk Assessment Tool



EXCEPTIONS:

- (1) Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a CE or a business associate (i.e. opening an incorrect chart);
- (2) inadvertent disclosure of PHI from one person authorized to access PHI at a CE or business associate to another person authorized to access PHI at a CE or business associate;
- (3) unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Attachment A (continued)

(1) Previously, the standard used by HHS for determining a breach was the “Risk of Harm” principle. This definition has been further clarified by HHS. The final rule kept the exceptions, but eliminated the harm standard.

HHS added language to the definition of “breach” to clarify that “an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, *demonstrates that there is more than a low probability* that the protected health information has been compromised.”

Instead of assessing the risk of harm to the individual, covered entities must assess the probability that the protected health information has been compromised based on a *risk assessment* that considers at least the following four factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

Three Exceptions

The final rule kept the three statutory exceptions to the definition of “breach”:

- A breach excludes any unintentional acquisition, access or use of protected health information by a workforce member (including volunteer or trainee) or person acting under the authority of a covered entity or business associate, if the acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule. “The exception does not, however, cover situations involving snooping employees, because access as a result of such snooping would be neither unintentional nor done in good faith,” HHS clarified.
- A breach excludes inadvertent disclosures of protected health information from a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity, business associate or organized health care arrangement in which the covered entity participates.
- Also exempted are disclosures of protected health information where a covered entity or a business associate has a good-faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. “For example, if a covered entity, due to a lack of reasonable safeguards, sends a number of explanation of benefits (EOBs) to the wrong individuals and a few of the EOBs are returned by the post office, unopened, as undeliverable, the covered entity can conclude that the improper addressees could not reasonably have retained the information,” HHS stated. “The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.”

Attachment B

Breach Notification Process

In the event the Breach Notification Risk Assessment determines a requirement to notify the affected individuals, and in the absence of a Law Enforcement Delay under Section 164.412, the Privacy Officer will designate an appropriate Company representative to proceed with the required notifications following these procedures in accordance with the appropriate level of notification as defined by HIPAA and the Breach Notification Rule:

- Select Medical will notify affected individuals following the discovery of a Breach and will provide this individual notice in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically. If Select Medical has insufficient or out-of-date contact information for 10-or-more affected individuals, Select Medical will provide substitute notice by either posting the notice at www.selectmedical.com or posting the notice in major print or broadcast media for the applicable jurisdiction(s). Individual notifications will be provided as soon as possible, in a time frame not to exceed 60 days following the discovery of a Breach. Individual notifications will include a description of the Breach, a description of the types of information involved in the Breach, the steps that affected individuals should take to protect themselves from potential harm, a brief description of what Select Medical is doing to investigate the Breach, mitigate the harm, and prevent further breaches, and contact information for Select Medical. All notifications, including substitute notice posted in print or broadcast media, shall provide a toll-free number for individuals to contact the covered entity to ask questions regarding the incident and to determine if their PHI was involved in a Breach.
- In the event of a Breach affecting more than 500 individuals, Select Medical will provide notice to major media outlets no later than 60 days following the discovery of the Breach. The media notice will provide the same information as an individual notice.
- In addition to notifying affected individuals and the media when appropriate, Select Medical will notify the U.S. Dept. of Health and Human Services Office for Civil Rights of the Breach. If the Breach affects 500 or more individuals, Select Medical will notify the Office for Civil Rights no later than 60 days following the Breach. If the Breach affects fewer than 500 individuals, Select Medical will notify the Office of Civil Rights on an annual basis, at least, and no later than 60 days following the end of the calendar year in which the Breach occurred.
- In incidents in which Select Medical is a Business Associate, Select Medical will notify the covered entity of the Breach to their PHI without unreasonable delay and no later than 60 days following discovery (unless the associated business associate agreement requires more specific notification time deadlines). Pursuant to the terms of the associated business associate agreement, Select Medical will provide the covered entity, to the extent possible, information regarding the identification of each individual affected by the Breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

Notification should include an apology and correcting the results of any inaccurate health information which was disclosed. The notification should also describe the type of information disclosed and how we are mitigating risk of harm. If the patient(s) personally identifiable information included social security number and date of birth, the notification will include a complimentary one year service with Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. Additional consideration should be given to provide information on the Federal Trade Commission's information on protection from identity theft. Correspondence may also include instructions on accessing the FTC website and phone number (www.ftc.gov/idtheft ; 877-382-4357). A copy of the FTC "Deter, Detect, Defend" publication should also be provided. Prior to any notifications being sent, the Privacy Officer must approve the notification language (after consulting with appropriate Select Medical leadership). Lastly, applicable state information breach notification laws should be considered with regard to state specific requirements.



Audit Control

| | |
|--------------|--------------------------------|
| Number | H42-A |
| Policy Owner | Privacy Officer |
| Approved By | Privacy and Security Committee |

| | |
|--------------------|------------|
| Effective Date | 10/17/2013 |
| Last Revision Date | 1/27/2021 |
| Page | 1 of 1 |

PURPOSE

The scope of this policy covers the hardware, software and procedural mechanisms that will be implemented by Select Medical Corporation (Select Medical) to record and examine activity in information systems that contain or access electronic protected health information (ePHI).

To protect the privacy and confidentiality of our patients' ePHI and to comply with federal law, this policy applies to all Select Medical workforce members.

POLICY

Select Medical has adopted this policy to set forth the internal audit procedures for the security of ePHI.

PROCEDURES

Audit Control Mechanisms

1. Select Medical shall utilize a mechanism to log and store system activity for each system that contains or accesses ePHI.
2. Each system's audit log **must** include, but not be limited to, user ID, login date/time, and activity time. Audit logs **may** include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
3. System audit logs shall be reviewed as needed.

Audit Control and Review Plan

1. The audit logs shall be reviewed as needed.
2. Any potential threats or incidents must be reported to the Security Officer through the communication channels outlined in H26-A Reporting a Security Incident policy.
3. The Security Officer must investigate all reports of threats or incidents.



Information Security Policy

| | |
|--------------|---------------------------|
| Number | IT101 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 12.31.2011 |
| Last Revision Date | 07.04.2024 |
| Page | 1 of 7 |

PURPOSE

Information is a critical Company asset and as such must be protected from misuse, improper access, and delays in processing. It is imperative that the following policy be implemented and enforced to ensure the confidentiality, integrity, and availability of Company Information.

Company Information must be protected in a manner commensurate with its sensitivity, value and critical nature. Security measures must be employed regardless of the medium on which Information is stored (i.e., paper, PCs, Workstations, Mobile Devices, Removable Media, etc.), the systems which process it (i.e., PCs, networks, voice mail systems, etc.), or the methods by which it is moved (i.e., email, paper, face-to-face conversation, etc.).

SCOPE

This document applies to Select Medical, its subsidiaries and affiliated companies and all personnel accessing Company Property.

RESPONSIBILITY

Supervisors and managers are responsible for keeping all Workforce members informed of this policy. All Workforce members will be informed of this policy through new-hire orientation and annual compliance training thereafter and will be required to acknowledge and abide by the policy.

DEFINITIONS

Cardholder Data: Data elements specified within the most recent version of the Payment Card Industry Security Standards Council Glossary.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Company Property: All right, title and interest in or to the Hardware, Software, Information, or Data owned, leased, or licensed by the Company.

Corporate Confidentiality Statement (must be used verbatim): Note: The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have

received this communication in error, please notify us immediately by replying to the message and deleting it from your computer. Thank you.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Encryption: Encryption is the conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties.

Hardware: All tangible equipment and media used in the capture, storage, processing, transmission, and presentation of Information and Data, including, but not limited to workstations, endpoints, mobile devices, information storage media of any kind, information presentation products, medical devices, and network equipment.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the IS Solution Center.

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security Technology, Operations and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Mobile Device: Any iOS or Android device that is not a Workstation, but is used as an electronic computing and communications device which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information.

Non-sensitive Data: Data or Information that can be shared with all audiences without restriction or concern for disclosure.

Owner of Information: The individual or entity who has a vested interest in, who has been given the authority to allow access to, and who has the responsibility of maintaining the integrity of the Information.

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a "passphrase."

Personal Computer (PC): Any laptop, notebook, desktop, thin-client, smartphone or any other personal computing apparatus or device which is used to access, process or display information. This definition does not include computing devices operating as servers in a hardened, controlled access, secured data center.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as HIPAA PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, and cameras.

Sensitive Data: All PII, PHI, Cardholder Data and Proprietary Data.

Shadow IT: The use of IT-related Hardware, Software and or cloud services by a department or individual without first obtaining the appropriate approval(s) from Shared Services.

Shared Services: The main operational groups for the Company's executive, managerial, Human Resources, Communications, Operations, Procurement, Finance, Legal and Accounting, Information Services, Central Business Office and other relevant departments that provide enterprise-wide support.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

UserID: The unique identifier, protected by a changeable Password, which identifies each computer, application, and/or system user.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is Company policy that:

1. All Information and Software that processes Data (which include programs making up operating systems) are Company Property. Company forbids either the Information or the Software to be given to or viewed by anyone not authorized by Company.
2. Unless for an approved business process, no Information, Data, or Software shall be downloaded, transferred or otherwise made available to non-Company Hardware or any non-Workforce member without prior permission from Information Security through the Workforce member's immediate supervisor and senior leadership.
3. At minimum, the following steps shall be taken to protect Company Information:
 - a) Control and limit physical access to areas containing Information and/or Data processing resources, to essential personnel.
 - b) Provide only the level of access necessary (READ, MODIFY and or DELETE) to those Workforce members with the need to use the Information.
 - c) Provide necessary procedures to ensure that the transferal or termination of a Workforce member's access is in accordance with their roles and responsibilities within the Company.
 - d) Provide necessary tools to monitor and enforce security policies.
 - e) Implement and maintain documented procedures to impede or prevent Workforce members or third parties from tampering with or misusing Information.
4. All Company Property shall remain the property of Company, regardless of its origin, including, but not limited to, any Software or Data developed by Workforce members for Company or using Company Property. The Workforce member hereby assigns to Company the entire right, title, and interest in and to any Software or Data developed by the Workforce member for Company, and shall execute any assignments or other documents necessary to effect such assignments. The Workforce member agrees that any Software or Data developed by the Workforce member for Company or using Company Property shall be deemed a "work made for hire".
5. No electronic devices connected to Company Property, including but not limited to broadband, dial-up, VPN, or SSL connections from remote locations, shall be left unattended while signed-on unless Password protected.
6. Each Workforce member must ensure that remote connections to Company assets are logged off when not in use and not left unattended unless Password protected.
7. While using Company Property, connections to the internet must not be left unattended, and internet browsers should be closed when not in use.

8. All remote connections should require the user to enter a UserID, Password and where feasible, two-factor authentication to gain access, and should not make use of any type of feature that would bypass this requirement unless a feature is specifically approved by the Chief Information Officer or Chief Information Security Officer.
9. Remote and/or local area network layer connections to Company's internal network resources are only permitted from Hardware owned by Company, unless authorized by Information Security.
10. Connecting any device or cloud service not issued, or previously approved, by Information Services to any Company Workstation, even for the purposes of providing power, is prohibited, unless authorized by Information Security. If these, or any other Shadow IT activities are identified, Company has the right to block such activities and enforce disciplinary action as deemed appropriate by Company.
11. When on Company premises the Workforce member shall not use or install any personal locks on any Hardware, safes, or storage cabinets, or on any adjacent office equipment. Company reserves the right to inspect the Workforce member's work area and remove, by any means, any personal locks found to be installed in violation of this policy.
12. When working remotely, personal locks may be used in order to lock and store Company Information away from unauthorized individuals. This can be via room, closet, drawers or cabinet.
13. The Workforce member shall be solely responsible for any Workstation activity conducted under the Workforce member's UserID, and shall not disclose such UserID and associated Password to anyone, unless authorized beforehand by a member of Information Security. The Workforce member shall not in any way attempt to discover the Password of any other Workforce member.
14. The Workforce member shall not use any Company Property, in whole or in part, for personal reasons, unless authorized by the Workforce member's immediate supervisor.
15. Testing of security systems is prohibited without approval of the Chief Information Officer or Chief Information Security Officer. Disclosing, capturing, altering, or destroying Information that relates to or creates security exposures is prohibited. All security exposures must be disclosed to the Chief Information Officer or Chief Information Security Officer as soon as possible. Additionally, Workforce members are prohibited from disclosing, changing, or disabling any audit features without the approval of Information Services.
16. Workforce members must report all system errors/issues with Company owned assets or systems to the I.S. Help Desk.
17. The Workforce member shall not use any Company Property to gain unauthorized access to any Software or Data, whether the property of Company or a third party.
18. The Workforce member shall not unduly influence or attempt to influence Company to purchase, lease, or license any Hardware, Software, or Data from a third party vendor with which the Workforce member has had prior dealings.
19. Workforce members should not expect privacy with respect to any use of or access to Company Property. Company reserves the right and has the legal authority to review any Data files, web or application activity, messages, or communications sent, received, or stored on Company Property. Workforce members will adhere to applicable laws and

- industry standards while utilizing Company equipment wherever they are physically located, including when they are on Company Property or working remotely.
20. The environments containing Company Information and Data processing resources shall be adequately protected by using appropriate procedures and technology. Some examples of these would be locked doors or cabinets, fire alarms, suppression devices, and emergency power supplies.
 21. All departments that process and maintain Company Information shall ensure that a documented contingency plan is developed to enable the continued availability of important or critical Information in the event of an extended emergency.
 22. Unless it has specifically been designated as Non-sensitive Data, all Company Sensitive Data must be protected from disclosure to third parties. Third parties may be given access to Company Sensitive Data only when demonstrable need-to-know exists, when a Company contractual agreement has been signed, and when such a disclosure has been expressly authorized by the relevant Company Owner of such Data. If Sensitive Data is lost, or disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, Information Security and Compliance must be notified immediately.
 23. All Workforce members who secure Company Property with Passwords or Encryption shall turn over the Passwords or decryption keys to Information Security upon separation from Company.
 24. If remote access to Company's internal network resources is granted, the Workforce member must maintain a work environment that meets security and confidentiality requirements for interacting with Sensitive Data as defined by Company's policies and procedures as well as established law. Workforce members must not compromise the confidentiality or security of Information due to remote Workstation access. Workforce members must ensure that Sensitive Data in any form cannot be accessed, viewed and/or heard by any unauthorized person. It is the Workforce member's responsibility to be aware of their surroundings when viewing, or discussing, Sensitive Data regardless of location.
 25. Any paper and or notes generated for work need to be properly shredded. If working remotely it is preferable that the paper or notes generated for work be taken to a Company location and placed in a shred bin.
 26. Breaches in the use and handling of Sensitive Data or technology, whether intended or unintended, will be subject to disciplinary action up to and including termination, in accordance with Company's Human Resources policies, procedures and Code of Conduct.
 27. The Workforce member shall use any Software purchased, leased, or licensed from third party vendors strictly in accordance with the license agreement and copyright statements for such Software. The Workforce member shall not copy, download or upload any such Software without the prior approval of Information Security, and shall not under any circumstances modify any such Software.
 28. The Workforce member acknowledges that any action taken by the Workforce member in violation of this policy may subject both the Workforce member and Company to criminal and civil liability. In the event that any suit, claim, or demand is asserted against Company which arises out of the Workforce member's actions in violation of this policy, the Workforce member shall indemnify, defend, and hold harmless Company from and

against all liability, cost, or expense, including attorney's fees. The indemnity contained herein shall survive the expiration or termination of the Workforce member's employment with Company.

29. Workforce members must follow all Company IT policies and HIPAA policies, in addition to this Information Security policy, in order to appropriately protect Company Information.

The Workforce member acknowledges that any violation of the above rules, aforementioned policies and procedures may subject the Workforce member to disciplinary action, including, but not limited to, termination of the Workforce member's employment and civil and criminal proceedings. In the event that the Workforce member's employment is terminated, the Company shall retain all legal or equitable remedies against the Workforce member, and such remedies shall be cumulative and not exclusive.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.



Electronic Communications Policy

| | |
|--------------|---------------------------|
| Number | IT102 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 12.31.2011 |
| Last Revision Date | 10.23.2024 |
| Page | 1 of 6 |

PURPOSE

The purpose of this policy is to ensure that all Workforce members are knowledgeable about the capabilities of electronic forms of communication and understand the circumstances in which these forms of communication are appropriate and permitted.

SCOPE

This policy applies to all Workforce members and any other individuals with authorized access to the Company network, and applies to all forms of Electronic Communications, including, but not limited to, web browsing, file transfers (FTP), file sharing, fax, electronic collaboration tools, artificial intelligence solutions, chat bots, virtual assistants, instant messaging, text messaging and e-mail.

RESPONSIBILITY

It is the responsibility of all managers to determine the forms of Electronic Communications that their staff requires to fulfill their job responsibilities, and to supervise their staff to ensure that they are utilizing Electronic Communications in accordance with the guidelines of this policy.

It is the responsibility of all Workforce members to utilize only those Electronic Communications for which they have been authorized. Workforce members using Electronic Communications must safeguard Company Information by understanding and complying with this policy and the related guidelines, as well as all other policies of the Company. Additionally, Workforce members are responsible for reporting breaches of this policy to Information Services or to their managers or supervisors, whichever is appropriate.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Company Property: All right, title and interest in or to the Hardware, Software, Information, or Data owned, leased, or licensed by the Company.

Corporate Confidentiality Statement (must be used verbatim): Note: The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any

dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to the message and deleting it from your computer. Thank you.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Electronic Communication: The transfer of Company Information and or Data via any electronic methods including, but not limited to, web browsers, file transfers (FTP), fax, electronic collaboration tools, artificial intelligence solutions, chat bots, virtual assistants, instant messaging, text messaging and e-mail.

Endpoint Security Software: Software including, but not limited to, AV/EDR that is installed on Workstations for the purposes of providing security assurance.

Firewall: Any hardware and/or software used to examine network traffic and control the flow of data between networks.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the I.S. Solution Center.

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Owner of Information: The individual or entity with a vested interest who is responsible for maintaining the integrity of, and access to, the information.

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a "passphrase."

Payment Card Industry (PCI) Data: Credit and debit card information, such as card validation codes, PINs, and full track data from the magnetic stripe.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as HIPAA PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Remote Connection: A connection to the Company network by an authorized Workforce member from an external network by way of VPN, HTTPS, SSL or other approved method.

Sensitive Data: All PII, PHI, PCI Data and Proprietary Data.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

UserID: The unique identifier, protected by a changeable Password, which identifies each computer, application, and/or system user.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is Company policy that all forms of Electronic Communication be utilized only by Workforce members who have been properly authorized. Electronic Communications are Company Property and their primary purpose is to facilitate Company business. Every Workforce member has a responsibility to maintain and enhance Company's public image and to use Electronic Communications in a productive manner. All outbound e-mail must include the Corporate Confidentiality Statement. Company will hold Workforce members accountable for

their individual behavior associated with Company name and all their activity conducted with Company Property.

The following items represent a set of minimum requirements that must be observed during any use of Electronic Communication. No Sensitive Data shall be sent via electronic means without first being properly secured following requirements within this policy.

1. Every effort must be made to protect Company Property. Workforce members must comply with the *Code of Conduct* when utilizing Electronic Communications.
2. All Workforce members must have Company's standard approved Endpoint Security Software properly installed and running on their Workstations. Workforce members are prohibited from disabling or removing any Endpoint Security Software from Company Workstations.
3. All Workforce members must be vigilant in watching for suspicious emails, ensuring that they do not open suspicious emails or click on any links within a suspicious email. Workforce should never forward a suspicious email to anyone outside of the U.S. Help Desk or Information Security. The appropriate way for all Workforce to report a suspicious email is via the Report Suspicious Email button in Microsoft Outlook or Outlook Web Access. Common traits of a suspicious email may include:
 - a) Generic "from" email addresses (e.g., helpdesk@support.com)
 - b) Subject lines containing words such as "Urgent" or "Alert"
 - c) Spelling mistakes
 - d) Warning banner at the top of the email
 - i. **WARNING: This email originated from outside the organization. Please validate the sender's email address and do not click links or open attachments unless you recognize the sender and are expecting the message.**
4. To effectively control and monitor Remote Connections, access will be allowed only via approved Software or approved remote access solutions by Information Security.
5. Sensitive Data may be sent via e-mail or over the internet only when it fulfills a valid business purpose. Sensitive Data should be labeled as such and its distribution must be tightly controlled (e.g., Password protect the document containing Sensitive Data and add the word "Encrypt" to the email subject line, double check to ensure that the person you are sending the Information to is the correct and appropriate recipient, always ensure that any Sensitive Data is shared with the minimum necessary recipients).
6. Documents and all other types of internal Information are Company Property and must not be sold nor transferred to any non-Company party for any purposes other than business purposes expressly authorized by the Company Owner of Information.
7. Security systems are in place that will monitor and record Workforce member usage of Company Property, including but not limited to web-site activity, e-mail, and file transfers, telephone and cellphone logs and instant message logs. This Information will be periodically reviewed by Information Security for possible misuse of Company Property and or unauthorized access.
8. Company reserves the right to examine e-mail, directories, files, and any other Information stored on Company Property. The examinations will be done to ensure compliance with policies, support the performance of internal investigations, and assist

with the management of Company Information systems. Company designated security personnel have the right to access and monitor all messages and files on Company Property.

9. Company supports strict adherence to Software vendor's licensing agreements. When using Company Property, copying of Software that violates the vendor's license agreement is prohibited. Obtaining Software through illicit means is prohibited. Reproductions of writings posted or otherwise available over the internet must be done only with the permission of the author/owner.
10. Electronic Communication must be in compliance with applicable federal, state and local laws and regulations. Use of Company Property for criminal purposes is prohibited, (i.e., materials that are of a fraudulent, defamatory, harassing, obscene, abusive, or threatening nature, or to solicit or exchange copies of copyrighted Software).
11. Workforce members must refrain from expressing personal opinions when using Company Property, except in a business context relating to trade associations and other professional activities.
12. While using Company Property, connections to the internet must not be left unattended, and internet browsers should be closed when not in use.
13. Use of personal e-mail to conduct business is strictly prohibited, including but not limited to forwarding of Company email to personal email.
14. Company has the right to access and disclose the contents of any Workforce member's Company Property as required for legal, security and audit purposes, and for legitimate Company operational purposes.
15. In an effort to protect Workforce members from unwanted or malicious e-mail or website activity, e-mail messages containing various types of attachments and content are filtered and not allowed to be received by Workforce members.
16. When using video conferencing solutions Workforce members should protect the privacy of themselves and others by:
 - a) Not attending meetings in areas where Sensitive Data may be overheard or seen on your screen by others in your vicinity.
 - i. If this is not possible, speakerphone should be disabled and headphones should be used. Workstation privacy screens should also be considered.
 - b) Enabling the virtual background, or blur background feature.
 - c) Closing all unnecessary applications, emails and documents prior to screen sharing
17. Unacceptable use of Electronic Communications includes, but is not limited to:
 1. Excessive or inappropriate personal use (e.g. conducting side business, playing games, solicitation to employment opportunities, electronic snooping or eavesdropping, gossiping via Electronic Communication systems).
 2. Using pay-per-call (900 number) services or international calling for non-work related activities.
 3. Allowing another person to utilize your UserID and Password to gain access or using another person's UserID and Password to gain access.
 4. Representing yourself as someone else.
 5. Accessing or distributing Information with illegal, racist, sexist, sexually-oriented, obscene, harassing, or other potentially objectionable content.

6. Disclosing inappropriate or Sensitive Data regarding the Company or its Workforce.
7. Soliciting or distributing malicious Software.
8. Distributing or storing harassing messages, chain letters, jokes, solicitations, offers to buy or sell goods, or other non-business material of trivial, frivolous, or otherwise unauthorized nature.
9. Maligning any other person or company.
10. Entering online forums or discussion boards for unauthorized or non-business purposes.
11. Inappropriately providing others with Information concerning Workforce members.
12. Interfering with the operation of the internet gateway, Firewalls, Endpoint Security Software or any other Software required by Information Services.
13. Engaging in illegal, fraudulent, or malicious conduct.
14. Monitoring or intercepting the files of Workforce members or third parties.
15. Obtaining unauthorized access to any Company Property.
16. Spamming e-mail accounts from Company e-mail services or any Company Workstations.
17. Texting Sensitive Data via unapproved solutions and or devices.
18. Furthering any kind of conduct that is deemed inappropriate or prohibited in the workplace or any other use that does not constitute Company business.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

Code of Conduct



Data Center Physical Security Policy

| | |
|--------------|---------------------------|
| Number | IT104 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 04.08.2014 |
| Last Revision Date | 10.23.2024 |
| Page | 1 of 5 |

PURPOSE

The purpose of this policy is to define the physical security measures that are in place to secure Company Data Centers.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies and to all Workforce members and visitors of the Company.

RESPONSIBILITY

It is the responsibility of the Data Center manager to ensure that the provisions in this policy are in place and appropriately adhered to by all Workforce members.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Company Property: All right, title and interest in or to the Hardware, Software, Information, or Data owned, leased, or licensed by the Company.

Corporate Offices: A building or group of buildings that serve as main base of operations for the Company's executive, managerial, Human Resources, Communications, Operations, Procurement, Finance, Legal and Accounting, Information Services, Central Business Office, Regional Business Office, and other relevant departments that provide enterprise-wide support, also known as Shared Services.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Data Center: A building, dedicated space within a building or a cloud tenant that supports computing services and Information Technology (IT) systems for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of Company Data.

Hardware: All tangible equipment and media used in the capture, storage, processing, transmission, and presentation of Information and Data, including, but not limited to workstations, endpoints, Mobile Devices, Information storage media of any kind, Information presentation products, Medical Devices, and network equipment.

HVAC: Heating, ventilation and air conditioning.

Information: All processed, organized, structured, and/or contextualized data that may be captured, stored, processed, or transmitted.

Piggybacking: When an unauthorized individual follows an authorized individual into a restricted area.

PIN: A personal identification number (PIN) is a numeric and/or alpha numeric security code for verifying an individual's identity.

Power Distribution Unit (PDU): A device used for controlling electrical power in a Data Center.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

Data Center Access:

Badge access to the Data Center shall only be authorized through an electronically documented request by the Workforce member's manager. This request must be submitted to the Data Center manager and must contain the following:

1. Business justification for access.
2. Requestor's functional responsibilities.
3. A specific request for approval of any of the following activities:
 - Observation / walk-through.
 - Front of rack access.
 - Physical shutdown / restart of Hardware.
 - Back-of-rack / Data cabling.
 - Rack / un-rack / move of Hardware.
 - Power grid / PDUs.
 - Escort of others who do not have access.

Failure to identify any specific activity(ies) for which approval is being requested will result in the assignment of observation and escort access only.

4. Unless authority is properly requested, and subsequently approved by the Data Center manager for the above activities, an individual may not be granted access to the Data Center and may not engage in any Data Center related activities, except as a guest in an observation role only.

Data Center access is reviewed quarterly by Data Center management. An individual's access may be removed due to any of the following:

1. Inactivity.
2. Lack of sufficient business justification for ongoing access.
3. Termination or voluntary separation from the Company.
4. Data Center access rules and responsibilities, or policies and standards are not adhered to.
5. Expiration of time-bound access.

Data Center Access Rules and Responsibilities:

Authorized individuals who are granted access to the Data Center must acknowledge and comply with Company's rules and responsibilities identified in this section. If a Data Center is hosted in a facility not owned and managed by Company, then any superseding rules, responsibilities, and/or restrictions specific to that location will also require compliance. Failure to comply may result in loss of Data Center access privileges.

1. No food or drink of any type is permitted in the Data Center.
2. No shipping containers of any kind, including cardboard boxes and packing materials, are permitted inside the Data Center. All equipment must be unboxed prior to entering the Data Center.
3. The authorized individual must observe and adhere to the *IT101 Information Security Policy* and *IT113 Change Control Policy*.
4. Company-owned Data Center: Individuals without Data Center access must be signed in and escorted by a Workforce member with appropriate access, and any such visit must be communicated to the Data Center manager or, in their absence, a Data Center analyst with as much advance notice as possible. Failure to do so may result in access not being authorized to such individuals.
5. Hosted Data Center: All access to the Data Center must be pre-approved based on the requirements for secure access to a site at the specific location. No unplanned access will be permitted.
6. Authorized individuals must prevent Piggybacking by remaining aware of their surroundings and ensuring that they are the only individual entering the Data Center unless one of the following is true:
 - a) they are escorting another individual with the approval of the Data Center manager or a Data Center analyst.
 - b) the authorized individual is an authorized Data Center escort.
7. Activities within the Data Center shall be restricted, as much as reasonably possible, to the area where the specifically approved actions are to take place.

8. Any authorized individual entering the Data Center is required to report to the Data Center manager or one of the Data Center analysts all apparent problems, or suspicious activity, within the Data Center and/or all violations of any Data Center policies or procedures.

Physical Access Controls:

1. Data Center doors are forcible entry resistant, self-closing doors. Alerts such as invalid badge attempts are logged in the badge system. Logs are reviewed on an as-needed basis by the Data Center manager.
2. All Company employees and third parties shall wear personal identification such as Company identification or visitor badges.
3. A video monitoring system records activity within the Data Center, including the points of access and the Data Center raised floor space.
4. Data Center access must, at a minimum, require one of the following:
 - a. A valid badge swipe at facilities where a PIN is not required.
 - b. A valid badge swipe and PIN at facilities where a PIN is required.

Environmental Monitoring of the Company-owned Data Center

1. Data Center manager is responsible for monitoring and upkeep of installed power conditioning, backup power generators, HVAC controls, moisture control, and temperature control systems in the Data Center.
2. Data Center is equipped with properly maintained fire detection systems, fire suppression systems, and fire alarm systems that automatically alert those who have responsibility for the Data Center in which each system is installed.

Company-owned Data Center Equipment and Facility Maintenance

1. The Data Center manager must approve all maintenance and service of Data Center infrastructure, which includes power generation and distribution, cooling, heating, fire suppression, and moisture detection systems, as well as room and facility modifications.

Acknowledgement of this policy is required to gain and retain access to Company Data Centers. Data Center management has the right to require additional training and/or acknowledgment of Data Center policies and/or procedures in order to obtain or retain access.

Violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy

documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

IT101 Information Security Policy

IT113 Change Control Policy



Corporate Physical Security Policy

| | |
|--------------|---------------------------|
| Number | IT105 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 04.08.2014 |
| Last Revision Date | 10.23.2024 |
| Page | 1 of 3 |

PURPOSE

The purpose of this policy is to establish the Company’s rules for granting, monitoring, and removing physical access at, and to, the Company’s Corporate Offices to protect assets, property and Data from misuse, improper access and theft.

SCOPE

This policy applies to all Company Corporate Offices and all persons conducting business at Company Corporate Offices including, but not limited to, Workforce members.

RESPONSIBILITY

It is the responsibility of all Workforce members to adhere to and report any violations to this policy.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Corporate Offices: A building or group of buildings that serve as main base of operations for the Company’s executive, managerial, Human Resources, Communications, Operations, Procurement, Finance, Legal and Accounting, Information Services, Central Business Office, Regional Business Office, and other relevant departments that provide enterprise-wide support, also known as Shared Services.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Human Resources (HR): The internal Shared Services department responsible for Workforce related matters including, but not limited to, recruiting and staffing, compensation and benefits, payroll, training and employee relations.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Piggybacking: When an unauthorized individual follows an authorized individual into a restricted area.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

It is the policy that:

1. Physical security systems must comply with all applicable federal, state, and local regulations including, but not limited to, building and fire prevention codes.
2. Physical access to all Company Corporate Offices must be managed using the Company approved badge access system.
3. Access to Company Corporate Offices must be restricted only to those personnel whose job responsibilities require access.
4. Authorized personnel must prevent Piggybacking by remaining aware of their surroundings and ensuring that other individuals do not enter the Company Corporate Offices without scanning their own badge.
5. Authorized individuals should stop any person they see in the Company Corporate Offices that does not have the appropriate approval as confirmed via Company identification, visitor badge, or appropriate escort, and direct them to the Corporate Offices front desk if applicable.
6. Temporary badges must be set with an expiration date that is aligned with the amount of time the access is needed.
7. The process for granting physical access to Company Corporate Office facilities must include the approval of the requestor's manager or supervisor, or be done as part of the Human Resources onboarding process.
8. Access badges, keys, and passcodes must not be shared with or loaned to others. The owner of the access badge, key or passcode will be responsible and liable for all activity.
9. Access badges should not be visible within photographs posted online.
10. Access badges, keys, and passcodes must be returned to management, Human Resources, or Information Services once they are no longer needed, or employment or contractual services have been terminated.
11. Badges/keys must not be allocated to another individual because it bypasses the return and request processes required.
12. If an individual changes positions within the organization or ends their working relationship with the Company, their physical access must be altered or terminated to

reflect their new status. It is the responsibility of the Workforce member's manager or supervisor to notify Human Resources to adjust access.

13. Lost or stolen access badges/keys must be reported immediately to management, Human Resources, or Information Services.
14. Corporate Offices that allow access to visitors will track visitor access using a sign-in/sign-out log and visitors must wear and visibly display their assigned visitor's badge at all times. Visitor's badges must be obtained at the Corporate Office front desk.
15. Badge access records and visitor logs for Corporate Offices will be retained for at least three (3) years and will be reviewed on an as-needed basis by Information Services.
16. Badge holders are not permitted to alter, modify or disfigure Company-issued badges.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.



Encryption Policy

| | |
|--------------|---------------------------|
| Number | IT106 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 03.23.2016 |
| Last Revision Date | 10.23.2024 |
| Page | 1 of 6 |

PURPOSE

The purpose of this policy is to define the standards to which Company adheres to when encrypting Electronic Communications and Information resources.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for the implementation and enforcement of this policy. Workforce members are responsible for adhering to the guidelines specified within this policy.

DEFINITIONS

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Certificate Authority: An entity that issues digital certificates accrediting the ownership of a public key by the named subject of the certificate.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Company-Owned Mobile Device: Any Mobile Device issued or owned by the Company.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Electronic Communication: The transfer of Company Information and or any Data via electronic methods including, but not limited to, web browsers, file transfers (FTP), fax, electronic

collaboration tools, artificial intelligence solutions, chat bots, virtual assistants, instant messaging, text messaging and e-mail.

Encryption: Encryption is the conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties.

File Encryption: The encryption of an individual file.

Full Disk Encryption: The encryption of all sectors of a storage device including removable media, whether hard disk drive, solid state drive, or other storage medium, to include unused and empty sectors.

Information: All processed, organized, structured, and/or contextualized data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Medical Device: As defined via Section 201(h) of the Food, Drug & Cosmetic Act, a medical device is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part of accessory which is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease or intended to affect the structure or any function of the body.

Mobile Device: Any iOS or Android device that is not a Workstation, but is used as an electronic computing and communications device which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information.

Multi-Factor Authentication (MFA): Verifies identification by combining a UserID and Password (something you know) with cell phone or landline (something you have).

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a "passphrase."

Payment Card Industry (PCI) Data: Credit and debit card information, such as card validation codes, PINs, and full track data from the magnetic stripe.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited

to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as HIPAA PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, and cameras.

Sensitive Data: All PII, PHI, PCI Data and Proprietary Data.

UserID: The unique identifier, protected by a changeable Password, which identifies each computer, application, and/or system user.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

Encryption Standard

Company uses Federal Information Processing Standard (FIPS) approved algorithms for Encryption of Data-at-rest and Data-in-motion. All Encryption methodology changes must be approved by the Chief Information Security Officer or Chief Information Officer.

Data-in-Motion

All Sensitive Data leaving the internal LAN/WAN must be encrypted. Encryption of Sensitive Data communications within the internal LAN/WAN is not required, but recommended. Supported methods of encrypting Data-in-motion include, but are not limited to:

- Hypertext Transfer Protocol Secure (HTTPS).
- Transport Layer Security (TLS).
- Secure File Transport Protocol (SFTP).
- Secure Socket Layer (SSL).
- Secure Shell (SSH).
- WiFi Protected Access (WPA).
- Virtual Private Networks (VPN).

Encryption for Data-in-motion is required for, but is not limited to, the following scenarios:

- Connections to Company WiFi.
- Remote access to Company internal resources including Workstations and Information.
- Sensitive Data transferred/communicated with destinations outside of Company network.

Email Encryption

When an email, regardless of what Data it includes, is sent outside of the Company network, Company's email solution uses opportunistic TLS encryption to secure the Data in transit.

If the external recipient accepts TLS, the email will be received with no further action required by the sender or the recipient.

If the external recipient does not accept TLS, and Company data loss prevention solution determines the email contains Sensitive Data, the email will be secured behind Company's email portal, where the recipient must register with a UserID and Password in order to receive the email.

If the external recipient does not accept TLS, and Company data loss prevention solution determines the email does not contain Sensitive Data, the email will be sent unencrypted with no further action required by the sender or the recipient.

Out of an abundance of caution, even though the technology employed automatically attempts to encrypt all Data sent externally, typing "Encrypt" or "Secure" in the subject line is a way to manually ensure that encryption occurs despite the technology's detection of the presence of any Sensitive Data. It is for this reason that Workforce members should still type "Encrypt" or "Secure" within the subject line when they are sending email outside of the Company that contains Sensitive Data.

Data-at-Rest

Full Disk Encryption is required for, but is not limited to, the following devices:

- All Company Workstations with the ability to store Data.
- Removable Media containing Sensitive Data approved by Information Security.

- All Company-Owned Mobile Devices.

If a Workstation, Mobile Device, Removable Media device or Medical Device cannot be encrypted due to technical limitations, the asset must be reported to Information Security for review. Where appropriate, Information Security will collaborate with other teams and subject matter experts to provide a recommendation of how to remediate the issue. If remediation is not feasible, the asset must be replaced by one that can meet Encryption requirements or be approved by the Chief Information Security Officer or Chief Information Officer.

Enforcement

Company ensures that devices and media are encrypted through one, or a combination, of the following measures:

- Automated policy enforcement.
- Automated inventory system.
- Compliance monitoring.
- Manual record keeping.

Key Management

Cryptographic keys will adhere to the following requirements:

- Cryptographic keys and public key certificates are generated within an issuing system or Certificate Authority.
- Keys are stored in centralized locations and must be secured by Multi-Factor Authentication.
- Access to stored keys is restricted to authorized individuals.
- Keys may be revoked, withdrawn, or deactivated when they have reached their natural date of expiry, they have been compromised, or when they are no longer needed for continuation of business processes (i.e. when an individual leaves the Company or a device has been decommissioned).

The process for recovering encrypted Information in the event of lost, compromised, or damaged keys will follow the steps required by the encrypted repository in question.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory

requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.



Identity and Access Management Policy

| | |
|--------------|---------------------------|
| Number | IT107 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 05.27.2008 |
| Last Revision Date | 3.4.2024 |
| Page | 1 of 5 |

PURPOSE

The purpose of this policy is to establish Identity and Access Management measures and requirements for protecting Information and Information systems against unauthorized access including identification, authorization and authentication of users, programs and processes that access Company Information and/or resources.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security or designee(s) are responsible for facilitating the creation, modification and removal of user accounts and access. Information Services (IS) is responsible for generating system access and role lists for review and recertification of access by an authorized approver or supervisor. All Workforce members are required to adhere to the guidelines specified within this policy.

DEFINITIONS

Access Provisioning: The creation, management and maintenance of a user's rights and privileges in one or more applications or systems.

Active Directory: A centralized service that facilitates authentication, permissions, domain and access management for interconnected network resources.

Administrative Accounts: Approved accounts that are assigned to individuals or systems for the sole purpose of performing job functions requiring elevated privileges.

Authoritative Record: A trusted, complete and accurate representation of available information that is validated in terms of authenticity, integrity, reliability and usability.

Business Partners: Any organization that has a contractual relationship to provide any product or service to the Company.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

De-provisioning: The removal, suspension or disabling of a user's rights and privileges in one or more systems or applications.

Governance, Risk and Compliance (GRC): Governance, Risk and Compliance (GRC) is the internal Information Security team that provides comprehensive IT risk assessments and compliance programs that empower risk based strategy and minimizes risk exposure of IT operations while simultaneously enabling business objectives.

High Risk Application: An application that interacts with or contains Sensitive Data, is available outside of the Company network and does not have the standard automated access termination controls.

Identity and Access Management (IDM): The internal Information Security team responsible to facilitate enterprise operations by securely and, wherever possible, automatically maintain minimum access necessary to all applications used by all workforce members, and those who support them.

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (IS): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

I.S. Help Desk: A team of dedicated resources who provide Workforce members with information and support related to the Company's IT systems. Also known as the I.S. Solution Center.

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a "passphrase."

Role-based Access: A method of defining and regulating access to computer systems, applications or network resources based on the roles of individual users within an enterprise.

Access Management

- User access shall be granted based upon the principles of need-to-know, least-privilege, and Role-based Access. Access not explicitly permitted shall be denied by default.
- User, system and application access must be processed through *IT201 User Access Request (UAR) Procedure* and tracked by Information Security. UARs must be submitted for the following:
 - A new user requires access that was not automatically provisioned for the purpose of fulfilling job responsibilities.
 - An existing user has a change in job function requiring a change in role and privileges that were not automatically provisioned or de-provisioned.
 - Termination of a Workforce member.
- The UAR will enforce the following requirements:
 - Access granted shall be limited to the systems and applications described on the request.
 - The request must be approved, at least, by the user's manager. Secondary and tertiary approvals may be required depending on the application and/or access being requested.
- When a Workforce member is terminated, access to systems and applications shall be automatically terminated through the Company's IDM solution or manually terminated by Information Security when prompted by a termination UAR or other automated and auditable means within monitored and audited performance service level agreement timelines.

Security Controls

- System and application Password complexity is required to meet strong authentication requirements and must align to requirements outlined in *IT114 Password Management Policy*.
- Encrypted, Virtual Private Network (VPN) solutions are implemented for Workforce members, contractor or third party remote access to the Company's network in accordance with *IT106 Encryption Policy*, and access properly logged.
- Remote access by vendors and Business Partners is managed and maintained through an approved vendor remote access solution.
- All remote access by vendors and Business Partners (e.g. remote maintenance) is disabled/deactivated when no longer required.
- Additional strong authentication methods such as multi-factor authentication are implemented, where possible, for all remote access to the Company's network and applications.

Audit and Management Review

- Information Services (IS) shall implement processes to enforce periodic user access reviews to be performed by Information/Data owners or designee(s) to ensure the following:
 - User access levels are appropriate.

- Terminated employees do not have active accounts.
- There are no group accounts, unless approved by management.
- Periodic reviews of user access will be conducted based on the following:
 - Recertification of identified High Risk Applications.
 - Internal compliance controls (e.g. Sarbanes-Oxley).
- User access lists will be generated for review with, at a minimum, the following Information for each Workforce member:
 - User ID.
 - Description.
 - Access Level.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

IT106 Encryption Policy
IT114 Password Management Policy
IT201 UAR Procedure



Firewall Policy

| | |
|--------------|---------------------------|
| Number | IT108 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 12.07.2010 |
| Last Revision Date | 07.04.2024 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to establish a set of requirements for the deployment and configuration of all Firewalls that process Company network traffic.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security and Firewall Administrators are responsible for ensuring proper Firewall installation, configuration, maintenance, Backup, restoration, and support. All Information Services leadership is responsible for enforcing the requirements defined in this policy. Workforce members are responsible for adhering to this policy.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Change Advisory Board: Governing body of I.S. management responsible for reviewing and approving enterprise Infrastructure and Application Software Changes.

Data Center: A building, dedicated space within a building or a cloud tenant that supports computing services and back-end Information Technology (IT) systems for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of Company Data.

Emergency Change: An unplanned change introduced to avoid, respond to, or resolve a problem or Major Incident that is causing, has caused, or could cause a service interruption.

Firewall: Any hardware and/or software used to examine network traffic and control the flow of data between networks.

Firewall Administrator: A company role varying between “modify” and “read-only” in privilege, and granted to those whose responsibilities may include, but are not limited to, Firewall installation, configuration, maintenance, backup, restoration, and/or support.

Hardware Firewall: A Firewall appliance or server attached to a network for the purpose of controlling traffic flow to and from single or multiple hosts or networks.

Host Firewall: Software-based Firewall, running on a single computer or server, with the ability to restrict network traffic only for that system.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Normal Change: A general purpose change type that requires one or more approvals.

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a “passphrase.”

Request Form: Request form outlining and describing a proposal for an introduction, alteration or removal of a product, system or service to/from the environment.

Standard Change: A change template that has been pre-approved and created by the Change Advisory Board.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

It is Company policy that:

1. All new Firewall installations and implementations must be approved by Company’s Information Security management team and must conform to the standards outlined in this policy. Unauthorized or non-approved Firewall implementations are prohibited and

may be subject to immediate removal, confiscation, and/or termination of network connectivity.

2. All Hardware Firewalls must be physically secured using, at minimum, a badge reader or lock-and-key.
3. Requests for Firewall Administrator privileges must follow *IT201 UAR Procedure* and be authorized and approved by Company's Chief Information Security Officer, Chief Information Officer or Vice President where segregation of duties applies.
4. Network Firewalls must be logically secured using, at minimum, Password authentication as outlined in *IT114 Password Management Policy*.
5. All Firewalls must be configured to deny all inbound and outbound traffic by default unless expressly permitted by a Firewall Administrator for an approved business or security purpose.
6. Any Firewall rules and/or configuration changes must be requested using the appropriate Request Form located on the Company intranet, including documentation, and approved prior to implementation. Configuration changes can only be conducted by a Firewall Administrator.
7. Firewall rules and configuration changes must only allow traffic as necessary for business operations. Firewall Administrators will perform quarterly reviews of such rule and configuration changes for the main Firewalls within the Company Data Centers to ensure they are still necessary for business operations.
8. Emergency Changes can be made by the Information Services application and systems teams in order to respond to a system or business risk prior to completing a Request Form and outside of previously approved change windows when necessary.
9. All changes must adhere to *IT113 – Change Control Policy*.
10. All business-critical Network Firewall configurations must be backed up nightly to an alternate storage location. Backup configurations will conform to *IT111 Backup and Retention Policy*. Access to Backup configurations is restricted to Firewall Administrators and Backup operators.
11. Firewall event and administration logs must be copied and retained in an alternate storage location in accordance with *IT111 Backup and Retention Policy* and *C09-A Document Retention Schedule*.
12. Firewall event and administration logs are reviewed as needed by the Firewall Administrators.
13. Exceptions to this policy will be handled on a case-by-case basis by the Chief Information Officer or Chief Information Security Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

IT111 - Backup and Retention Policy
IT113 – Change Control Policy
IT114 – Password Management Policy
IT201 – UAR Procedure
C09-A Document Retention Schedule



Removable Media Policy

| | |
|--------------|---------------------------|
| Number | IT110 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 04.21.2011 |
| Last Revision Date | 08.28.2024 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to establish the requirements governing the use of Removable Media devices for business purposes.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for enforcing the requirements outlined in this policy. All Workforce members are responsible for the proper use and safeguarding of Removable Media devices used for business purposes.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery, or may refer to a single Electronic Data copy. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Encryption: The conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the IS Solution Center.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as HIPAA PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Read Only Access: The ability to read, retrieve and copy electronic data.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, and cameras.

Sensitive Data: All PII, PHI, and Proprietary Data.

Service Request (SR): A user request for a standard change, order, or for access to an Information Services (I.S.) service.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

Write Access: The ability to read, retrieve, write, modify, and delete electronic data.

POLICY

It is the Policy of Company that:

1. Default configuration for all Company-issued Workstations will permit Read Only Access to Removable Media devices and deny Write Access.

2. Workforce members must submit a Service Request for Write Access privileges by contacting the I.S. Help Desk or utilizing the self-service option on Company's intranet portal.
3. Write Access privileges will be granted on a per-Workstation basis, usage should be limited to the minimum length of time necessary for legitimate business purposes and privileges must be approved by Information Security.
4. The storage of Sensitive Data on Removable Media devices is strictly prohibited, unless otherwise necessitated by legitimate business processes and permitted by Information Security.
5. Removable Media devices containing Sensitive Data MUST be encrypted in compliance with the *IT106-Encryption Policy*.
6. Workforce members must follow the *H04-A Safeguarding Protected Health Information Policy* when storing Sensitive Data on Removable Media devices.
7. Company prohibits the use of Removable Media devices as a Backup solution for files, unless otherwise approved by Information Security.
8. All use of Removable Media devices for business purposes must comply with the *IT101-Information Security Policy*.
9. Removable Media devices that are returned to Information Services must be sanitized in accordance with the *IT112-Data Sanitization Policy*.
10. All Removable Media devices must be kept physically secure. When not in use, Removable Media devices should be stored out of plain view, on one's person, or in a locked drawer or room.
11. In the event that a Removable Media device is lost or stolen, it must be reported immediately to Company's Information Services department via the I.S. Help Desk and a Lost Stolen Asset Form must be submitted in accordance with *IT202.1 – Lost Stolen Asset Form*.
12. Exceptions to this policy will be addressed on a case-by-case basis by the Chief Information Officer or Chief Information Security Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

H04-A-Safeguarding Protected Health Information Policy
IT101-Information Security Policy
IT106-Encryption Policy
IT112-Data Sanitization Policy
IT202.1 – Lost Stolen Asset Form



Backup and Retention Policy

| | |
|--------------|---------------------------|
| Number | IT111 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|-------------|
| Effective Date | 11.26.2014 |
| Last Revision Date | 10.23.20234 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to establish the Company's requirements for secure Backup and Retention of Electronic Data.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for establishing corporate security requirements for the secure Backup and Retention of Electronic Data. Information Services (I.S.) is responsible for ensuring that Backup and Retention practices meet the defined security requirements, and that all Backup and Retention activities are in alignment with Company requirements as determined by Company, Governance, Risk and Compliance (GRC), and the appropriate I.S. support team(s). In all cases where Backup services are provided by either Company or by Company vendors, I.S. management is responsible for enforcing this policy.

DEFINITIONS

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery, or may refer to a single Electronic Data copy. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Backup Frequency: How often a Backup occurs, usually defined and managed in a program that can set and enforce the defined schedule. The number of Backups or series of Backups that is intended to represent, be reassembled into, or be a component of a full copy of the Electronic Data for an application or service taken on a continuous, hourly, daily or monthly interval.

Business Partners: Any organization that has a contractual relationship to provide any product or service to the Company.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Data Center: A building, dedicated space within a building or a cloud tenant that supports computing services and back-end Information Technology (IT) systems for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of Company Data.

Disaster Event: An event of any unplanned cause that results in the loss of application or system access and/or data to an extent that an alternative site or alternative infrastructure must be utilized to provide access to the unavailable application(s), system(s) or data.

Disaster Recovery (DR): Process of attempting to return the business to a state of normal operations either at an interim minimal survival level and/or re-establishing full-scale operations.

Electronic Data: A general term for all data and metadata that is recorded or transmitted electronically.

Governance, Risk and Compliance (GRC): Governance, Risk and Compliance (GRC) is the internal Information Security team that provides comprehensive IT risk assessments and compliance programs that empower risk based strategy and minimizes risk exposure of IT operations while simultaneously enabling business objectives.

Hardware: All tangible equipment and media used in the capture, storage, processing, transmission, and presentation of Information and Data, including, but not limited to workstations, endpoints, mobile devices, information storage media of any kind, information presentation products, medical devices, and network equipment.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, and cameras.

Retention: The act of storing and maintaining copies of Electronic Data in a retrievable form, for any period of time beyond initial Backup.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

POLICY

It is the policy of Company that:

1. Production Electronic Data must be backed up using tools, procedures, Software and Hardware in such a way that will meet Disaster Recovery (DR) requirements as defined in *IT119 Disaster Recovery Policy*. Electronic Data must be able to be recovered using the established recovery plan documents for the Electronic Data, provide near-term restore as required by Company, and meet all security requirements defined for Backup of Electronic Data.
2. Backups must be identifiable in such a way that recovery or restore to an available point in time is easily determined. The movement and location of all Backup Removable Media must be continuously updated and remain current.
3. Removable Media for Backups must be physically stored in secure locations. All storage locations must be approved by the Chief Information Officer.
4. Access to Backups is restricted to I.S. staff based on job function. Access to Backups may be granted to approved Business Partners for various purposes related to Removable Media handling, Disaster Recovery testing, Data erasure, media conversion, Data migration, or Hardware upgrades.
5. All Backups must be on Company-owned assets, or on assets provided by an approved Backup services Business Partner specifically identified to hold Backups, or on Data storage provided as a Company approved vendor cloud storage offering. No Backups may be placed on employee-owned devices or employee contracted cloud storage.
6. All cloud-based Backup services provided by Company chosen Business Partners must be adequate and appropriate and allow Company to remain in compliance with its internal requirements and policies.
7. Backups must be encrypted according to the requirements of the *IT106 Encryption Policy*.
8. Backup Frequency will be determined by either business, application or system defined requirements.
9. Exceptions to this policy must be reviewed and approved by the Chief Information Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

C09-A-Document Retention Schedule

H22-A-Record Retention Schedule

IT105-Corporate Physical Security Policy

IT106-Encryption Policy

IT119-Disaster Recovery Policy

Select Medical Disaster Recovery Plan

Concentra IS Disaster Recovery Plan



IT Asset Data Sanitization Policy

| | |
|--------------|---------------------------|
| Number | IT112 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 11.24.2014 |
| Last Revision Date | 08.28.2024 |
| Page | 1 of 3 |

PURPOSE

The purpose of this policy is to establish Company’s requirements regarding Data disposal and sanitization of Company owned Information Technology (IT) Assets.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

It is the responsibility of all Workforce members to ensure that all IT Assets are sent to the I.S. Asset Management team for disposal and sanitization. The I.S. Asset Management team is responsible for ensuring the secure disposal and sanitization of IT Assets.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Data Sanitization: Process of permanently removing and/or rendering unrecoverable, Data stored on Company-owned assets, including but not limited to computers, laptops, backup tapes, Removable Media and/or disks, in accordance with guidelines outlined in *NIST 800-88 rev 1 Special Publication Guidelines for the Sanitization of Media*.

Encryption: The conversion of electronic Data into another form, which cannot be understood by anyone except authorized parties.

End of Life: A state of a product’s lifecycle where it is no longer maintained or supported by the manufacturer.

I.S. Asset Management: The internal Information Services team responsible for creating and maintaining the Company’s centralized processes and procedures to ensure technology assets are deployed, tracked, and retired in a controlled manner.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security

program including, but not limited to Security, Technology, Operations, Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Information Technology (IT) Asset: A piece of Company Hardware and or Software.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Sanitized Information Technology (IT) Asset: Company Information Technology (IT) Asset that has undergone the Data Sanitization process and contains no recoverable Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

It is the Policy of Company that:

1. IT Assets must be encrypted in adherence with the *IT106-Encryption Policy*, whenever possible.
2. IT Assets containing Data must undergo the Data Sanitization process if the IT Asset is no longer required for business use, the IT Asset is to be repurposed for a different use within the Company, or if the IT Asset has reached End of Life.
3. All Company IT Assets must be returned to the I.S. Asset Management team for Data Sanitization in accordance with the *IT117-IT Asset Return and Management Policy*.
4. Upon the I.S. Asset Management leadership team's approval, any Company IT Asset that is eligible for sale or donation must undergo the Data Sanitization process.
5. Any Company IT Asset that is being repurposed, recycled, or permanently retired must undergo the Data Sanitization process by authorized members of Information Services or authorized third parties who are previously approved by I.S. Asset Management and Information Security.
6. Sanitized IT Assets must not contain usable residual Data, and the Data purged from the IT Asset must not be recoverable.
7. All IT Assets must have Company identifying marks removed prior to disposal.
8. Company will conform to guidelines outlined in *H04-A-Safeguarding Protected Health Information (PHI)* and *HIPAA Security Rule: 45 CFR 164.310(d)(2)(i) and (ii)* in regards to sanitizing IT Assets involving PHI.

9. Authorized third parties are required to provide a certificate of data destruction and a certificate of proper disposal in accordance with the U.S. EPA.
10. Unauthorized disposal of IT Assets is strictly prohibited.
11. Exceptions to this policy will be addressed on a case-by-case basis by the Chief Information Security Officer or Chief Information Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

H04-A-Safeguarding Protected Health Information (PHI)

IT106-Encryption Policy

IT117-IT Asset Return and Management Policy

NIST 800-88, rev 1 Special Publication Guidelines for the Sanitization of Media

HIPAA Security Rule: 45 CFR 164.310(d)(2)(i) and (ii)



Password Management Policy

| | |
|--------------|---------------------------|
| Number | IT114 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 03.23.2016 |
| Last Revision Date | 3.4.2024 |
| Page | 1 of 3 |

PURPOSE

The purpose of this policy is to define Password requirements, the protection of those Passwords, and the frequency of Password changes for all Company assets.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for ensuring the implementation and enforcement of this policy. Workforce members are responsible for the proper use and protection of their Password and must adhere to the guidelines listed within this policy.

DEFINITIONS

Administrative Accounts: Approved accounts that are assigned to individuals for the sole purpose of performing job functions requiring elevated privileges.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Domain Security Policy: A set of rules applied to computer and/or user Active Directory accounts for the purpose of protecting all devices and users on that domain.

Multi-Factor Authentication: Verifies identification by combining a username and Password (something you know) with cell phone, landline or token (something you have), and or a biometric factor like fingerprint or facial characteristics (something you are).

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a "passphrase."

Standard Accounts: Are unique accounts assigned to a Workforce member or service for the purpose of authenticating to various systems and resources.

UserID: The unique identifier, protected by a changeable Password, which identifies each computer, application, and/or system user.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is the Policy of the Company that:

- A. For all applications, services or UserIDs that authenticate via Active Directory, Passwords should adhere to Domain Security Policy with the following requirements:
 1. Must be at least 8 characters in length.
 2. All Passwords must contain 3 of the following 4 categories.
 - a. Must contain at least one upper case letter (e.g., A-Z).
 - b. Must contain at least one lower case letter (e.g., a-z).
 - c. Must contain at least one number.
 - d. Must include at least one special character.
 3. May not contain your UserID.
 4. Password must not match the last 24 passwords used.
 5. Password belonging to Standard Accounts and Administrative Accounts must expire every 90-days.
 6. All Select Medical domain accounts must automatically lock after 5 consecutive incorrect login attempts within the threshold defined in the default Domain Security Policy.
 7. All Concentra domain accounts must automatically lock after 10 consecutive incorrect login attempts within the threshold defined in the default Domain Security Policy.
 8. All locked accounts can only be unlocked by an Administrative Account or by authorized self-service tools.
 9. Locked accounts must undergo user verification by an Administrative Account prior to the account being unlocked.
- B. When possible, all applications, services or UserIDs that do not authenticate via Active Directory shall be configured to use the above Password requirements. Any exceptions to the Password requirements must be approved by the Chief Information Officer or Chief Information Security Officer.
- C. All Workforce members are expected to adhere to the following requirements:

1. Unique initial Passwords must be provided through a secure and confidential manner and those initial Passwords must subsequently be changed upon first logon.
 2. Vendor-supplied initial default and/or blank Passwords must be reset in alignment with the requirements detailed in this policy upon installation of application, device, or operating system.
 3. Passwords are only to be used for legitimate access to networks, systems or applications related to performing Workforce job duties; Company Passwords must never be re-used for any non-work purposes or to access any non-Company related systems (i.e. Facebook).
 4. Passwords must not be disclosed to other Workforce members or individuals for any reason.
 5. Passwords must not be written down, posted, or exposed in an unsecured manner such as on a notepad or posted on a Workstation.
 6. Passwords must not be displayed in plain text when entered into a system or application.
 7. Passwords must not be sent to a non-Company email address. Information Security, in its sole discretion, will monitor for Passwords being sent to non-Company email addresses and escalate instances of non-compliance as appropriate.
- D. Password policies of new joint ventures and acquisitions will be evaluated within the first 90 days of formalized partnership or ownership. If remediation is required, a plan will be documented.
- E. Where feasible, Multi-Factor Authentication should be used in combination with a Password.
- F. Any exceptions to this policy must be approved by the Chief Information Officer or Chief Information Security Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.



Anti-Malware Policy

| | |
|--------------|---------------------------|
| Number | IT115 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 10.21.2015 |
| Last Revision Date | 08.28.2024 |
| Page | 1 of 3 |

PURPOSE

The purpose of this policy is to identify which systems require Anti-Malware and standardize Company's minimum Anti-Malware requirements.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for ensuring the implementation and enforcement of this policy. Workforce members should inform Information Security about any Workstation not compliant with this policy.

DEFINITIONS

Anti-Virus (AV)/Endpoint Detection & Response (EDR): A program, software, appliance or service that monitors a Workstation or network to identify malware to prevent, contain or alert on malware incidents.

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery, or may refer to a single Electronic Data copy. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the IS Solution Center.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Malware: Any software or code designed to infiltrate or damage a computer system or network without the owner's informed consent. These include but are not limited to computer viruses, worms, trojan horses, spyware, adware, and ransomware.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is the Policy of Company that:

1. Where possible, all Company Workstations must have Company approved AV/EDR Software installed which can be maintained through a centralized console and will be administered by Information Security.
2. AV/EDR detection engine and pattern library files must be kept up to date automatically without user interaction.
3. Workforce members are prohibited from tampering with or making changes to, including disabling Company AV/EDR Software. All efforts must be made to protect the AV/EDR Software from tampering.
4. Information Security will monitor AV/EDR compliance on all applicable Workstations connected to Company network in accordance with *IT308 – Microsoft Windows Endpoint and Server Compliance Standard*.
5. Information Security must be notified by any Workforce member via a support ticket to the I.S. Help Desk regarding any observed conflicts encountered between Company AV/EDR and other installed Software.
6. Email servers must have either an external or internal AV/EDR scanning application that scans all email destined to and from the email server. Local AV/EDR scanning applications may only be disabled during Backups if an external AV/EDR application still scans inbound emails while the Backup is being performed.
7. Company shall maintain logs of AV/EDR scans where possible for 13 months and review on an as-needed basis.
8. Exceptions to this policy must be reviewed and approved by the Chief Information Officer or Chief Information Security Officer.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

References and Related Documents

IT308 – Microsoft Windows Endpoint and Server Compliance Standard



Cybersecurity Incident Response Policy

| | |
|--------------|---------------------------|
| Number | IT116 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 02.02.2016 |
| Last Revision Date | 08.28.2024 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to ensure that a security incident response program is maintained in the event that a Cybersecurity Incident is discovered within the Company.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Information Security is responsible for ensuring the implementation and enforcement of this policy. Information Security will supply the resources needed and collaborate with other subject matter experts as necessary to appropriately address identified Cybersecurity Incidents. It is the responsibility of all Workforce members to report any actual or potential threats or violations that may affect the confidentiality, integrity or availability of Company Data, Software or Workstation directly to the Privacy or Security Officer, HIPAA Question Line, HIPAA Help email, the I.S. Help Desk, or through any other Company compliance program reporting mechanism.

DEFINITIONS

Business Partners: Any organization that has a contractual relationship to provide any product or service to the Company.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Cybersecurity Incident: Actions taken through the use of an Information system or network that result in an adverse effect on an Information system, network, and/or the Information residing therein.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the IS Solution Center.

Incident Response Plan: An organized approach for detecting, responding to, and limiting the effects of a Cybersecurity Incident or breach and managing the impact of the incident.

Incident Response (IR) Team: A centralized function within Company that responds to Cybersecurity Incident(s).

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Security Breach: Any cybersecurity incident resulting in unauthorized access, modification and/or exfiltration of Company Data by bypassing security mechanisms.

Security Event: An observable change in the everyday operations of a system, network, application or information technology service indicating that a security policy may have been violated or a security safeguard may have failed.

Security Operations Center (SOC): A centralized function that continuously monitors and improves Company's security posture while also responding to Cybersecurity Incidents.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

Company will establish and maintain a security incident response program to address Cybersecurity Incidents, including but not limited to theft, misuse of Data, intrusions, hostile probes, and malicious Software. All Cybersecurity Incidents must be reported as soon as practicable in accordance with *H26-A Reporting a Security Incident*. The following are examples of methods for discovering and reporting a Cybersecurity Incident:

Discover:

- A Cybersecurity Incident reported by any member of the Workforce.
- A Cybersecurity Incident reported by the Privacy Officer, Security Officer, Compliance or Privacy team, or any member of the Privacy and Security Committee.
- A Cybersecurity Incident reported by the SOC or Incident Response (IR) team.

- Notification from a third-party such as a Business Partner, vendor, government agency, or Information sharing organization.

Report:

- Contact the Select Medical I.S. Help Desk (888-972-1199).
- Contact the Concentra I.S. Help Desk (877-327-2771).
- Phone call, email or other form of electronic communication directly to any member of Information Security.
- Email the Privacy or Security Officer (privacyoffice@selectmedical.com or infosecurity@selectmedical.com).
- Call the HIPAA Question Line (717-730-4230).
- Contact the HIPAA Help email (HIPAAHelp@selectmedicalcorp.com).

Information Security will respond to and coordinate with other Company departments and third-parties as necessary to investigate scenarios that include, but are not limited to, the following, when appropriate:

- Unusual or apparently malicious use of Information assets.
- Malicious code (viruses, worms, or other malicious Software).
- Unauthorized Information access, usage or disclosure.
- Unauthorized physical access and usage.
- Any Cybersecurity Incident whereby a Workforce member, either directly or by using a program, performs functions for which such Workforce member does not have authorization.
- Any actions involving the Company's applications, Information systems, Information, or electronic devices in violation of Company policy or applicable laws or regulations.

Information Security will test the *Incident Response Plan* annually via tabletop exercises, simulations or other comprehensive exercises to determine the effectiveness of the plan, opportunities for improvement, and document all results.

Following guidance from Company's legal department under attorney client privilege, the Information Security management team will provide notice of any Security Breaches to the Company's General Counsel following *H39-A Breach Notification*.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

H26-A Reporting a Security Incident

H39-A Breach Notification

Incident Response Plan



Business Continuity Policy – Shared Services

| | |
|--------------|---------------------------|
| Number | IT118 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 10.04.2018 |
| Last Revision Date | 3.4.2024 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to ensure that a Business Continuity Plan(s) and a Business Unit Plan(s) are maintained in the event that Company Corporate Offices suffers a major Business Disruption Event. An interruption to the operations of the Data Center is addressed in *IT119 Disaster Recovery Policy*.

SCOPE

This policy applies to Company Corporate Offices.

RESPONSIBILITY

Information Security is responsible for facilitating and documenting this policy. Each Business Unit is responsible for ensuring the implementation and enforcement of this policy and any other plans specific to that Business Unit. The Business Continuity Team will supply the resources needed and collaborate with other subject matter experts as necessary to appropriately address business continuity issues. It is the responsibility of all Workforce members to notify the Business Continuity Team of any Business Disruption Events defined in this policy.

DEFINITIONS

Business Continuity Plan (BCP): A comprehensive, proactive plan supporting the continuous operation of critical business functions that may include, or depend upon, lower level plans which support specific functions, departments, units, or areas of the business.

Business Continuity Planning Team: Individuals who own, contribute to, create and validate the BCPs.

Business Continuity Response Team: Individuals who are engaged to respond to a Business Disruption Event; this will generally include the affected BCP owner(s), Disaster Recovery Workforce and additional IT staff from applicable teams depending on the scenario as needed.

Business Disruption Event: An event of any unplanned cause, which may threaten the operations, Workforce, clients, brand image or reputation of the Company.

Business Unit: A separate division within the Company that often develops and implements its own processes independently from the core business or brand while still adhering to the overall Company policies.

Business Unit Plan: A comprehensive high-level plan outlining a department's response and related requirements to a Business Disruption Event or Disaster Event.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Compliance: The internal Shared Services department that ensures Company complies with applicable laws, regulations and rules in order to preserve the integrity and reputation of Company. Also known as Internal Audit.

Corporate Offices: A building or group of buildings that serve as main base of operations for the Company's executive, managerial, Human Resources, Communications, Operations, Procurement, Finance, Legal and Accounting, Information Services, Central Business Office and other relevant departments that provide enterprise-wide support, also known as Shared Services.

Cybersecurity Incident: Actions taken through the use of an Information system or network that result in an actual or potentially adverse effect on an Information system, network, and/or the Information residing therein.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Data Center: A building, dedicated space within a building or a cloud tenant that supports computing services and back-end Information Technology (IT) systems for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of Company Data.

Disaster Event: An event of any unplanned cause that results in the loss of application access and/or data to an extent that an alternative site or alternative infrastructure must be utilized to provide access to the unavailable application(s), system(s) or data.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations, and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

I.S. Help Desk: A team of dedicated resources who provide Workforce members with information and support related to the Company's IT systems. Also known as the I.S. Solution Center.

Recovery Point Objective (RPO): The maximum age of data that can be lost as the result of a Disaster Event, starting from the time of the event and looking backwards toward the most recent recoverable copy of that data.

Recovery Time Objective (RTO): The maximum tolerable length of time that an application can be down during a Disaster Event, before operation of the application is restored.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

Company will establish and maintain a Business Continuity Plan(s) and associated Business Unit Plan(s) to respond to and address Business Disruption Events and Disaster Events which includes, but is not limited to, weather-related events, significant property loss or damage, Cybersecurity Incidents, loss of utilities, and man-made disasters. Company will take all reasonable and appropriate steps necessary to protect its business, reputation, Workforce members, and the tangible (property) and intangible (intellectual property) resources used to execute key business processes.

As part of the Business Continuity Plan(s), the Business Unit Plan(s) will contain, at a minimum, the following information:

- Identification of critical business functions and processes needed to maintain operations during a crisis.
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for Disaster Events.
- Capacity planning, which includes the number of Workforce members needed to perform critical functions and when those functions need to resume.
- Roles and responsibilities.

All Business Disruption Events must be reported as soon as practicable. The following are examples of methods for reporting or becoming aware of a Business Disruption Event:

- Contact the Select Medical I.S. Help Desk (888-972-1199).
- Contact the Concentra Solution Center (877-327-2771).
- Phone call, email or other form of electronic communication directly to a member of the Information Services leadership team.
- Notification from a third-party such as a business associate, vendor, fire or police organization, or other emergency management agency.

The Business Continuity Team will coordinate with Information Security and infrastructure to respond to Disaster Event scenarios that lead to one of the following situations:

- The Corporate Offices are non-operational, but the Data Center is operational.

- The Corporate Offices are operational, but the Data Center is non-operational.
- Both the Corporate Offices and Data Center are non-operational.
- Inpatient and/or Outpatient facilities are not able to provide services.
- Identified critical third-parties are not available.

The Business Continuity Team shall test the Business Continuity Plan(s) and other related documents annually via plan walk-throughs, tabletop exercises, simulations or other comprehensive exercises to determine the Business Continuity Plan(s) effectiveness as well as Data and application criticality and document all results, which are shared with Compliance.

The Business Continuity plan(s) and other related documents are to be kept up-to-date and, at a minimum, will be reviewed on an annual basis.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

IT119 Disaster Recovery Policy
Select Medical Business Continuity Plan
Concentra Business Continuity Plan
Corporate Business Unit Continuity Plans
Inpatient Division Continuity of Operations Plan
Outpatient Division Continuity of Operations Plan
Select Medical Disaster Recovery Plan
Concentra IS Disaster Recovery Plan



Disaster Recovery Policy

| | |
|--------------|---------------------------|
| Number | IT119 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 01.22.2016 |
| Last Revision Date | 10.23.2024 |
| Page | 1 of 5 |

PURPOSE

The purpose of this policy is to define the Company's Disaster Recovery activities regarding the high-level process to recover IT systems, applications, and Data from any Disaster Event.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

The business and application support teams are responsible for defining service levels in conjunction with the annual business impact analysis and Business Continuity Plan(s) and updating processes as approved by the respective Business Units. The application and systems owners of the CMDB record are responsible to work with technical teams and vendors to define the Disaster Recovery Plans. Annual testing of the Disaster Recovery Plan(s) is the responsibility of the Disaster Recovery Coordinator and will be a collaborative effort by all applicable application owners.

DEFINITIONS

Application Availability and Recovery Definition (AARD): A conceptual metric comprised of the following recovery related measurements for each application or service: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These recovery related measurements may or may not be identified in all of the current tools used by Company for creating backup copies of Electronic Data, however, where they do exist, they will be considered guidelines for creating recovery plans.

Authorization List: List of Company employees approved by the Chief Information Officer on record with the Disaster Recovery provider(s) who can declare a Disaster Event.

Availability Assurance Testing: The periodic testing of the capability, processes, procedures and plans to enable the restoration of applications and services with the prescribed RPO and RTO to ensure compliance with the Disaster Recovery plan(s) and Business Continuity Plan(s) objectives.

Backup: The act of creating and saving a retrievable exact copy of Electronic Data to a storage device for the purposes of preventing loss and facilitating recovery. The backup may be immutable depending on the technology leveraged for creating and storing it. The purpose of the Backup is for use as a recovery source in a Disaster Event, or as a source for near term restore.

Business Continuity Plan: A comprehensive, proactive plan supporting the continuous operation of the critical business functions that may include, or depend upon, lower level plans, which support specific functions, departments, units, or areas of the business.

Business Unit: A separate division within the Company that often develops and implements its own processes independently from the core business or brand while still adhering to the overall Company policies.

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities controlled by Select Medical Corporation.

Configuration Management Database (CMDB): A database maintained by the Information Services department that is used by the Company to store information about hardware and software assets including the relationship between those assets.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Disaster Event: An event of any unplanned cause that results in the loss of application or system access and/or data to an extent that recovery efforts must be initiated and/or an alternative site or alternative infrastructure must be utilized to provide access to the unavailable application(s), system(s) or data.

Disaster Recovery: Process of attempting to return the business to a state of normal operations either at an interim minimal survival level and/or re-establishing full-scale operations.

Disaster Recovery Coordinator: Workforce member that coordinates the resources needed to recover the enterprise's systems and applications following a disaster. The Disaster Recovery Coordinator is also responsible for the annual Availability Assurance Testing.

Disaster Recovery Plan: A comprehensive, proactive plan supporting the process of restoring the infrastructure, connectivity or applications and systems that enable business to return to an acceptable state of operations.

Hardware: All tangible equipment and media used in the capture, storage, processing, transmission, and presentation of Information and Data, including, but not limited to

Workstations, endpoints, Mobile Devices, Information storage media of any kind, Information presentation products, Medical Devices, and network equipment.

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Recovery Point Objective (RPO): The maximum age of data that can be lost as the result of a Disaster Event, starting from the time of the event and looking backwards toward the most recent recoverable copy of that data.

Recovery Site: A location whose purpose is to house IT infrastructure that will be used to recover applications or services when a Disaster Event occurs. A Recovery Site can be a Company facility or a vendor-owned facility.

Recovery Time Objective (RTO): The target for the maximum tolerable length of time that a recovery plan can take to restore an application to operable status following a Disaster Event.

Service Restoration Plan (SRP): The documented procedure for restoring an application or business service back to a satisfactory level of operation after a Disaster Event or other significant outage. This is equally applicable to individual applications or the larger overall business service.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

POLICY

It is the policy of the Company that:

1. Company shall develop and maintain comprehensive Disaster Recovery Plan(s) to support Business Continuity Plan(s).
2. The CMDB is the repository for capturing the owner and RPO and RTO requirements defined for applications and services. All applications with RPO and RTO requirements significantly relevant to any Business Unit needs are expected to be included in the CMDB. Any applications that do not have RPO and RTO requirements listed in the CMDB will follow a default AARD. The default AARD shall be:
 - a) RTO – 72hours.
 - b) RPO – 24hours.
 - c) MAO – 96 hours.

3. IS Owners should maintain up-to-date Service Restoration Plan (SRP) documents where possible, that appropriately capture the steps that would be necessary to recover the application(s) and/or business services they are responsible for to an operational state following a Disaster Event.
4. The Disaster Recovery Plan(s) will contain, at a minimum, the following information:
 - a) Authorization List.
 - b) Identification of Disaster Recovery teams, defining their roles and responsibilities.
 - c) Requirements for planning and execution of Availability Assurance Testing.
 - d) Strategies for responding to specific technology incidents, as defined in the Business Continuity Plan(s).
 - e) Address critical technology elements, including systems, networks, databases and Data, in accordance with key business activities.
5. The Disaster Recovery Plan(s) will identify the current Recovery Sites. The Recovery Sites will serve one or more of the following:
 - a) High availability site that provides additional equipment for critical applications and services by providing appropriate replication or service redundancy; serving as a failover option to minimize downtime.
 - b) Cold sites that contain predetermined Hardware and Software configurations provisioned in the Disaster Recovery contract that are kept offline and can be brought online for testing and Disaster Events in an on-demand, as-needed basis.
 - c) Cloud services that provide capacity on demand, for testing and Disaster Events.
6. Disaster Recovery Plan(s) shall be periodically tested to ensure the systems, networks, databases and other infrastructure elements can be recovered or reestablished to an acceptable and adequate state in Disaster Events. These tests will also ensure that Workforce members understand how the plan is to be executed and are prepared to conduct their roles and responsibilities effectively in response to a Disaster Event.
7. The Disaster Recovery Plan(s) and other related documents are to be kept up-to-date and, at a minimum, reviewed on an annual basis.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

Select Medical Disaster Recovery Plan
Concentra IS Disaster Recovery Plan
Select Medical Business Continuity Plan
Concentra Business Continuity Plan



Data Classification Policy

| | |
|--------------|---------------------------|
| Number | IT123 |
| Policy Owner | Information Security |
| Approved By | Chief Information Officer |

| | |
|--------------------|------------|
| Effective Date | 1.25.2021 |
| Last Revision Date | 07.04.2024 |
| Page | 1 of 4 |

PURPOSE

The purpose of this policy is to define guidelines related to Data Classification, labeling, and handling to ensure that Information is protected in a manner commensurate with its sensitivity, value, and critical nature.

SCOPE

This policy applies to Select Medical and its subsidiaries and affiliated companies.

RESPONSIBILITY

Compliance is responsible for providing education to Workforce members on the appropriate application of this policy and associated practices. Information Security is responsible for implementing technical controls that assist the enforcement of this policy. All Workforce members are responsible for adhering to the guidelines specified within this policy.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Compliance: The internal Shared Services department, which includes Internal Audit, that ensures Company complies with applicable laws, regulations and rules in order to preserve the integrity and reputation of Company.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Data Classification: The process of sorting and categorizing Data into various types, forms or any other distinct class to identify the level of security and privacy protection to be applied.

Electronic Data: A general term for all data and metadata that is recorded or transmitted electronically.

HIPAA Compliance Training: Annual training and education courses including the latest threats and issues vital to maintaining the confidentiality, integrity, and availability of Sensitive Information, which are assigned to all Workforce members based on job function.

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security, Technology, Operations and Incident Response, Governance, Risk and Compliance, and Identity and Access Management.

Mobile Device: Any iOS or Android device that is not a Workstation, but is used as an electronic computing and communications device which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information.

Non-sensitive Data: Data or Information that can be shared with all audiences without restriction or concern for disclosure.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, backup tapes and cameras.

Retention: The act of storing and maintaining copies of Electronic Data in a retrievable form, for any period of time beyond initial Backup.

Sensitive Data: All PII, PHI, and Proprietary Data.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff

and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is Company policy that:

1. All Information is classified as one of the below categories:
 - Sensitive Data.
 - Non-sensitive Data.
2. Information can take many forms including, but not limited to, the following:
 - Hard copy Data.
 - Data stored electronically in computer systems, cloud, software as a service, and other hosting service environments.
 - Communications sent or received digitally or on hard copy.
 - Verbal communications.
 - Data stored on Removable Media.
3. All Workforce members are responsible for identifying and understanding proper Data Classification and for ensuring that commensurate protection, in accordance with *H03-A Workforce Obligations Policy* and the annual HIPAA Compliance Training, is applied to Data at all times.
4. If a Workforce member questions whether or not Information is Sensitive Data, they must default to treating it as Sensitive Data; at no time should Sensitive Data be handled in a manner that is not commensurate with its sensitivity, value, and critical nature.
5. As is detailed in the annual HIPAA Compliance Training, security measures to restrict unauthorized access or disclosure of Sensitive Data, both technical and physical, must be employed by all Workforce members regardless of the medium on which Information is stored or transmitted (i.e., paper, Workstations, Mobile Devices, CDs, tapes, etc.), the systems which process it (i.e., computers, networks, etc.), or the methods by which it is moved (i.e., electronic mail, paper, conversation, etc.).
6. Workforce members may not disable or inhibit security measures meant to protect Sensitive Data without first receiving permission to do so, on a temporary basis, by the Chief Information Security Officer or the appropriate manager within Information Security.
7. Any Workforce member requiring access to Sensitive Data beyond what is provisioned based upon role must submit a User Access Request (UAR) in accordance with *IT201 – UAR Procedure*.
8. For Information Retention and disposal, the following must be considered for all Information and Data:
 - It must be retained as outlined in *IT111-Backup and Retention Policy and H22-A Records Retention Policy*
 - It must be disposed of in accordance with *IT112-Data Sanitization Policy*.

A violation of this policy or of the standards, procedures or guidelines established in support of this policy may be considered grounds for disciplinary actions up to and including termination of employment.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.

REFERENCES AND RELATED DOCUMENTS

H03A-Workforce Obligations Policy
H04A-Safeguarding Protected Health Information Policy
H22A-Records Retention Policy
H29A-Information Access Management Policy
IT101-Information Security Policy
IT106-Encryption Policy
IT110-Removable Media Policy
IT111-Backup and Retention Policy
IT112-Data Sanitization Policy
IT201-UAR Procedure

EXHIBIT G
INFORMATION SYSTEMS AND TECHNOLOGY

1. Contractor will provide, install, configure, manage and support all equipment and clinical software systems used by Contractor employees, and will be responsible for appropriate training therewith. Contractor will be responsible for all licensing, maintenance, security, and support of any workstations, equipment, and service required for internet connectivity as follows:

- a. Connectivity: Applications require a full separate Contractor network and will be installed. Contractor will provide an Internet T1 or greater connection for the Contractor applications and hardware. County is responsible for the extension of the DEMARC (carrier hands off the circuit to Contractor) into the Onsite Center. County will provide a fully network communication wired facility, including Ethernet drop points located in the ceiling for wireless access points, if applicable. County will provide a labeled patch panel within two (2) feet of the network rack location.
 - i. If County desires to utilize its existing internet connection which is dedicated to the Onsite Center, then Contractor shall install a security/network appliance to create a secure IP sec VPN tunnel connection connecting to the Contractor network through the County internet in order to connect to the required software applications to perform the Services. County assumes primary responsibility for network performance and operation that impacts the Contractor Services at the Onsite Center. County assumes responsibility for any data breaches on its own network.
- b. Network/Electrical: The Onsite Center will include network and electrical ports above workspace counters in accordance with Contractor's specifications. If ports are located below workspace counter, County will provide corresponding holes to drop device cables.
 - ii. Network drops are to be clearly identified and labeled with port numbers correlating with the patch panel.
 - iii. Two (2) network ports per device and two electrical and network ports are to be no more than sixteen (16) inches apart and must be located greater than sixteen (16) inches from a water source (sink).
 - iv. Adequate number of electrical/network ports: Four (4) network ports per device and two (2) electrical outlets per workstation (1 workstation = 4 network ports and 2 electrical outlets).
- c. Space: Contractor will recommend the locations for all network ports based on hardware installation needs, determined either by site visit and/or clinic diagram(s).
 - i. Administrative workspaces must have adequate space to accommodate the following equipment: PC, monitor, keyboard, printer, scanner, and mouse, as well as space for the user to work. At a minimum, each administrative workspace shall be 28 inches (28") high, two feet (2') deep, and six feet (6') long.
 - ii. Exam rooms must have available empty wall space at least 24 inches (24") wide, floor to ceiling, containing network and electrical ports for wall-mounted workstations.
 - iii. It is recommended that the network and electric ports be no more than four feet (4') away from any workstation space in order to use standard network cables and surge protectors as priced.
- d. Telecommunications: County will provide all hardware and software for an Onsite Center phone system and IT support for the phone system. Further, County will provide at a minimum the following items:
 - i. Separate phone and facsimile lines
 - ii. Dedicated phone line for credit card machine for payment collection
 - iii. Ability to transfer to any phone
 - iv. Internal lines – select Contractor employee
 - v. Voice Mail – select lines

c. Disposition Upon Termination. Upon termination of this Agreement, Contractor will retain all Contractor owned equipment/hardware. However, County and Contractor may agree that such Digital X-ray equipment (the "X-ray") previously deployed to the Onsite Center is retained by the County. The X-ray and the accompanying CR PC will remain with the County and Contractor will dispatch a third-party vendor to the Onsite to re-image the CR PC and reload associated medical data to the device before final turnover of the X-ray to the County.