CARROLLTON
FOOT CENTER

HIPAA Compliance Manual

Carrollton Foot Center PLLC
4221 Medical Pkwy
Ste 450

Apr 02, 2018

Table of Contents

I. Introduction

General HIPAA Compliance Statement

The organization, Carrollton Foot Center, will be referred to hereafter as **PROVIDER.**

PROVIDER has adopted this HIPAA Compliance Policy Manual in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act ("ARRA")) and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

PROVIDER hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs General HIPAA Compliance for **PROVIDER**. All personnel of **PROVIDER** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- **PROVIDER** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **PROVIDER** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- It is the Policy of **PROVIDER** to become and to remain in full compliance with all the requirements of HIPAA.
- It is the Policy of **PROVIDER** to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
- All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with **PROVIDER**'s Document Retention policy.

Procedures

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **PROVIDER** commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- **Privacy Policies and Procedures** -- **PROVIDER** shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.

- **Privacy Personnel** -- **PROVIDER** shall designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on **PROVIDER**'s privacy practices.

- **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the **PROVIDER** (whether or not they are paid by **PROVIDER**). **PROVIDER** shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.

- **Sanctions** -- **PROVIDER** shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.

- **Mitigation** -- **PROVIDER** shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

- **Data Safeguards** -- **PROVIDER** shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.

- **Complaints** -- **PROVIDER** shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **PROVIDER** shall explain those procedures in its privacy practices notice.

- **Retaliation and Waiver** -- **PROVIDER** shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **PROVIDER** shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

- **Documentation and Record Retention** -- **PROVIDER** shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

Compliance and Enforcement

All **PROVIDER** managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **PROVIDER**'s Sanction Policy.

Statement of Intended Audience

The intended audience for this document includes individuals classified as employees, officers, and agents of PROVIDER. However, Business Associates, contractors, temporary staff, volunteers, and other third party affiliates are bound by and should duly comply with all parts of this policy at all times. Relevant portions of the policy should be communicated clearly as an expectation of compliance to the aforementioned parties.

II. Stakeholders

a. Privacy Officer

General Purpose: Pursuant to HIPAA and HITECH, every practice or healthcare organization must designate a Privacy Officer. The Privacy Officer may have other titles and duties in addition to his/her Privacy Officer designation in a typical practice or organizational setting. The Privacy Officer is responsible for the development and implementation of privacy policies and procedures, and shall oversee all ongoing activities related to the development, implementation and maintenance of the practice/organization's practices in accordance with federal and state laws.

i. Supervisor

The Privacy Officer reports to [Click to Edit] This could be the Head of the Practice, the Head of the Practice's Management Committee, Office Manager, Director, CEO, etc..

ii. Responsibilities

1. Develop and formulate policies and procedures that establish standards for privacy, giving specific guidance to all members of the workforce.

2. Assist management with implementation of the privacy policies and procedures to ensure compliance with applicable federal and state law.

3. Commission and participate in ongoing audits established to investigate and monitor compliance with privacy standards and procedures required by federal and state law.

4. Serve on the Compliance Committee and stay informed on current issues regarding privacy compliance; present written materials for discussion and action.

5. Maintain an awareness of laws and regulations, keeping abreast of current changes that may affect healthcare systems through personal research, seminars, training programs, and peer contact.

6. Maintain a system of management reporting that provides the system with timely and relevant information on all aspects of privacy compliance issues.

7. Oversees and ensures the right of the practice/organization's patients to inspect, amend and restrict access to protected health information, when appropriate.

8. Works with all practice/organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the practice/organization's policies and procedures and legal requirements.

9. Direct efforts to communicate and promote understanding of the components of the privacy standards, laws, and regulations, and consequences of noncompliant behavior through written materials and training programs.

10. Oversees, directs, delivers and ensures mandatory and ongoing education and training programs for all members of the workforce, including when material changes are made to the privacy policies and procedures.

11. Ensure that ***PROVIDER*** documents that training has been provided.

12. Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities, and serves as a resource for workforce members on privacy issues and questions.

13. Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy practices for all individuals in the practice/organization's workforce, extended workforces, and for all business associates, in cooperation with his/her immediate supervisor, Human Resources, the Security Officer and legal counsel, as applicable.

14. Periodically recommend revisions to the privacy policies and procedures in response to new or amended governmental laws, rules, or regulations.

15. Take steps to verify that Business Associates are (a) aware of and following appropriate PHI privacy and security policies and procedures and same are reflected in a written Business Associate Agreement; and (b) ensuring their Subcontractors (as that time is defined by 45 C.F.R. § 160.103) understand their responsibilities as to PHI privacy and security, and written Business Associate Agreements have been signed.

16. Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the practice/organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

17. Consult with legal counsel, as necessary, with regard to the privacy standards and other applicable federal and state law.

18. Serves as a member of, or liaison to, the organization's IRB or Privacy Committee, should one exist. Also serves as the information privacy liaison for users of clinical and administrative systems.

19. Submit an Annual Report to the Click here to enter text..

20. Cooperates with the U.S. Department of Health and Human Service's Office of Civil Rights, other legal entities, and organization officers in any compliance reviews, audits or investigations.

b. Security Officer

General Purpose: In compliance with the security regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, including the Health Information Technology for Clinical and Economic Health Act (HITECH), and good security practice, **PROVIDER** is responsible for appointing a HIPAA Security Officer. The Security Officer is responsible for developing and monitoring practices to ensure that the **PROVIDER**'s health information is secure from unauthorized access, protected from inappropriate alteration, physically secure, and available to authorized users in a timely fashion. The Security Officer, along with the Privacy Officer, is also responsible for the oversight and management of all activities related to the development, implementation, maintenance of, and compliance with the entity's policies, procedures, and standards governing the privacy, confidentiality, and security of all individually identifiable health information in compliance with HIPAA, HITECH, the U.S. Department of Health and Human Services regulations implementing HIPAA, HITECH, particularly the HIPAA privacy regulations, HIPAA and HITECH security regulations, and other state and federal laws, professional ethics, and accreditation standards protecting the confidentiality and privacy of individuals and their health and other information, such as financial information. The Security Officer's duties include training in and disseminating of security policies and practices and planning for timely resumption of access to information in the event of a serious disruption.

i. Supervisor

The Security Officer reports to [Click to Edit] This could be the Head of the Practice, the Head of the Practice's Management Committee, Office Manager, Director, CEO, etc.

iii. Responsibilities

1. Be a member of the **PROVIDER** management team to bring the entity into overall compliance with HIPAA and HITECH. Conduct gap analysis and risk analysis from security perspective.

2. Participate in the strategic planning of information security policies and procedures. Work with department heads, the **PROVIDER** Privacy Officer, risk management, quality assurance, human resources, and the legal department to ensure compliance with the security and privacy regulations and state and federal laws protecting patient confidentiality and privacy.

3. Provide leadership to HIPAA/HITECH committees, work groups, and others charged with oversight of the **PROVIDER** security and privacy program.

4. Work with the clinical staff and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the **PROVIDER**, its personnel, good medical practice, or proper health information management practices.

5. Work with the **PROVIDER** Privacy Officer to ensure appropriate coordination between the **PROVIDER**'s security program and its privacy program.

6. Monitor **PROVIDER** operations and systems for security compliance. Report to the Click here to enter text. on the status of security compliance.

7. Revise the security program as necessary to comply with changes in the law, regulations, professional ethics, and accreditation requirements and as necessary because of changes in patient/client mix, business operations, and the overall health care climate.

8. With other **PROVIDER** personnel, such as management, the legal department, and other related parties, represent the **PROVIDER**'s security interests with external parties who may attempt to enact or modify security and privacy protections to ensure that such laws or regulations do not unnecessarily adversely affect the **PROVIDER**.

9. Review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply.

10. Provide information on the **PROVIDER**'s security policies and practices for employees and others with access to health information Ensure that training conforms to existing policies and procedures.

11. In coordination with key personnel, develop and implement the following plans: information security disaster plan, emergency mode operation plan, backup plan, physical security plan, personnel security plan, access policies, and others. Test and revise plans as necessary to ensure data integrity, confidentiality, and availability.

12. Conduct at least annually, a security risk analysis and recommend and implement necessary modifications, changes and improvements to system policies and procedures, to ensure the integrity of the privacy of protected health information.

13. Develop, implement and monitor policies and procedures regarding the use of mobile devices, their security, loss procedures, and tracking methods.

14. Ensure that **PROVIDER** personnel have uninterrupted access to critical patient information in the event of a power outage, natural or manmade disaster, or other disruption.

15. Perform internal audit of data access and use to detect and deter breaches.

16. Receive reports of security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

17. Initiates, facilitates and promotes activities to foster information security awareness within the organization and related entities, and serves as a resource for workforce members on security issues and questions.

18. Maintain awareness of changes in security risks, security measures, and computer systems.

19. Consult with legal counsel, as necessary, with regard to the security standards and other applicable federal and state law.

20. Cooperates with the U.S. Department of Health and Human Service's Office of Civil Rights, other legal entities, and organization officers in any compliance reviews, audits or investigations.

Other Stakeholders

III. Privacy Policies

The HIPAA Privacy Rule in general and privacy policies specifically mandate and outline the safeguards that are necessary to be in place to protect patient's rights regarding protected health information ("PHI"). Privacy Policy establishes limits and conditions on what **PROVIDER** can do with patient data without explicit authorization.

Use and Disclosure of Protected Health Information Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.

PROVIDER is not required by Federal Privacy regulations to obtain patient's written consent prior to using or disclosing protected health information for the purpose of payment, treatment, health care operations, or to public health organizations if specific need arises.

PROVIDER is required to disclose protected health information if ordered by a court of law.

PROVIDER is required to protect all forms of protected health information regardless of transmission medium. PHI transmission mediums include, but are not limited to, oral conversation via telephone or voicemail, paper records, data in transit over the Internet, fax machines, volatile and non-volatile electronic storage.

PHI records may be de-identified if the following example identifiers are not present:

1. Names
2. All geographic subdivisions smaller than a state, including the physical address
3. All elements of dates (excluding the year) directly relating to an individual
    a. Birthdate
    b. Admission date
    c. Discharge date
    d. Date of death
4. Telephone number
5. Fax number
6. E-mail address
7. Social security number
8. Medical record number
9. Health plan beneficiary number
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web Univerisal Resource Locators ("URLs")
15. Internet Protocol ("IP") address
16. Biometric identifiers
17. Full face photographic images
18. Any other unique identify number, characteristic or code

PROVIDER is committed to the individual expectation of treatment and efficient payment for accurate support in the health care chain; which will require the use and disclosure of protected health information for purposes of treatment, payment and healthcare oversight.

<u>Treatment</u> is defined as

1. Provision, coordination or management of health care and related services among PROVIDER and other health care providers.
2. Consultation between PROVIDER and other health care providers and a specific patient
3. Referral of a patient between a health care provider and PROVIDER

<u>Payment</u> activity encompasses:

1. Actions by PROVIDER to obtain payment for services rendered or premiums entitled.
2. Determining eligibility under a plan
3. Risk adjustments
4. Review of services for coverage and justification of charges

5. Disclosures to consumer reporting agencies; limited to individual's payment history

Healthcare oversight are administrative, financial, legal and quality improvements necessary for PROVIDER to run its business, supporting the core functions above or treatment and payment. Activities included but not limited to this list are:

1. Activities relating to the creation, renewal, or replacement of health benefits
2. Conducting legal and medical reviews, auditing services, and compliance initiatives
3. Business planning and development
4. Conducting quality assessments and improvement activities

Minimum Necessary Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.

HIPAA requires that requests of protected health information ("PHI") be limited by the method of least privilege. The access granted to an employee of PROVIDER will be what is required as necessary to complete a specific job task or purpose.

PROVIDER must make reasonable efforts to limit PHI to the limited data set or minimum necessary to accomplish the intended purpose of use or disclosure while dealing with or requesting protected health information from another covered entity.

Minimum necessary does not apply to:

1. Disclosures to or requests by a health care provider for treatment purposes.
2. Disclosures to the individual who is the subject of the information.
3. Uses or disclosures made pursuant to an individual's authorization.
4. Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
5. Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
6. Uses or disclosures that are required by means law which compels PROVIDER to make use or disclose PHI in a manner enforceable by a court of law.

HIPAA requires that uses of protected health information be limited to only employees who are performing services to patients or health plan members and only for purposes allowed under the Privacy Rule. Only employees with responsibilities related to a particular patient or health plan member may access information pertaining to that individual and only the minimum necessary information should be accessed to perform the related work responsibilities

Request for Correction or Amendment of Protected Health Information

Patient information related to patient rights includes only that information contained in each patient's designated record set, in accordance with the requirements at § 164.501.

PROVIDER will assist patients with their right to amend protected health information contained in a designated record set, of which encompasses PHI but also billing records and other records PROVIDER uses to make decisions about a patient.

Information contained about a patient within the context of the designated record set must be made available to the patient or executor as necessary and appropriate.

Request for Restrictions of Protected Health Information

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning requests for restrictions of Protected Health Information, in accordance with the requirements at § 164.522.

PROVIDER must permit patients a means to request restrictions on protected health information. The restrictions request may be within the following scope:

1. Uses or disclosures of protected health information about the patient to carry out treatment, payment, or health care operations
2. Disclosures permitted under § 164.510(b)

PROVIDER is not required to agree to a restriction.

If PROVIDER agrees to a restriction, then only emergency treatment may supersede the agreement for the restriction and only for as long as is necessary to carry out the emergency treatment.

PROVIDER may terminate its agreement to a restriction under the following conditions:

1. Patient agrees or requests termination in writing
2. If by oral agreement, it must be documented
3. PROVIDER terminates the agreement, and only such information may be made available after the patient has been duly notified of the termination.

Request for Confidential Communication by Alternate Means or Alternate Location

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning requests for confidential communication of Protected Health Information, in accordance with the requirements at § 164.522(b).

PROVIDER must permit patients to request and must accommodate reasonable requests to make available communications of protected health information by an alternate means or at an alternative location.

PROVIDER may provide this request at the provision of handling of contact method and possible payment required to service request.

Request for an Accounting of Disclosures Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to the relative accounting of disclosures of patient records, in accordance with the requirements at § 164.528.

PROVIDER is required to make available patient protected health information records for a minimum of six years.

HIPAA maintains a subset of accounting disclosures which the patient may not or legally not be able to be provided information for as part of a request for disclosures:

1. To carry out treatment, payment, and health care operations as provided in §164.506
2. To individuals of protected health information about them provided in § 164.502
3. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502
4. Pursuant to an authorization as provided in § 164.508
5. For PROVIDER, INC's directory or to staff involved in a patient's care or other notification purposes as provided in § 164.510
6. For national security or intelligence purposes as provided in § 164.512(k)(2)
7. To correctional institutions or law enforcement officials as provided in § 164.512(k)(5)
8. As part of a limited data set in accordance with § 164.512(e).
9. Occurred prior to PROVIDER, INC's compliance date.

PROVIDER may be required to suspend a patient's rights to receive an accounting of disclosures involving a health oversight agency or law enforcement official as outlined in § 164.512(d) or § 164.512(f), for the time specified by the agency or official; if an agency or official provides PROVIDER with written statement attesting to the following:

1. Accounting request to the patient would likely impede an agency or officials activities
2. Specification of the time for which a suspension is required

In the event that a statement is made orally by a health oversight agency or law enforcement official, PROVIDER, INC will document and proceed as follows:

1. Document the statement, including the identity of the health oversight agency or law enforcement official making the statement.
2. Temporarily suspend the patient's right to an accounting of disclosures subject to the statement.
3. Limit the suspension to no longer than thirty (30) days from the date of the oral statement, unless within such time as an official written statement outlined as above is submitted.

i. Content of Accounting of Disclosures

PROVIDER will provide a written accounting of disclosures which at minimum must:

1. Include disclosures of protected health information that occurs during the six years (or shorter if patient requests a duration less than six years) prior to the date of the request, including disclosures made to or by a business associate.
2. The accounting must include:

    a. The date of disclosure
    b. Name of the entity or person who received the protected health information and address, if possible
    c. Brief description of the protected health information disclosed

d. Brief statement of the purpose for the disclosure of protected health information
e. If multiple disclosures are made to a single entity or person for the same purpose then PROVIDER may provide a statement of frequency, including the number of disclosures made during the accounting period and date of last disclosure, instead of multiple duplicate written disclosures.

3. PROVIDER must act on a patient's request for an accounting of disclosures no longer than sixty (60) days from the receipt of the request. At which time PROVIDER will:

    a. Provide the accounting of disclosures requested
    b. Extend the time required to produce documentation by thirty (30) days provided that:

        i. PROVIDER must provide a written statement for delay
        ii. PROVIDER will only request one such extension.

4. If, during the period of accounting, PROVIDER had made disclosures of protected health information for a particular research purpose as outlined in § 164.512(i) for 50 or more patients, the accounting for disclosures may provide:

    a. The name of the research activity
    b. Simple English description of the research activity, including purpose of the research and criteria for selecting candidates
    c. Brief description of the protected health information disclosed
    d. Date, including interval for which the disclosures occurred, including date of last disclosure
    e. Name, address, phone number or the entity that sponsored the research and researcher to whom the information was disclosed.

    If it is reasonably likely that a patient's protected health information was disclosed to a research entity, at the request of the patient, PROVIDER will assist in contacting the research entity and responsible researcher.

Disclosure to Law Enforcement Policy

PROVIDER may disclose a patient's protected health information to law enforcement provided a valid authorization is received executed by the individual whose information is in question or the request must fall within circumstances under both HIPAA and state law which allows the disclosure of protected health information without an authorization. Such requests must be scrutinized by the Privacy Officer and the following are exceptions to the rule:

1. To prevent or lessen a serious or imminent threat to the health or safety of a patient or the public.
2. It is believed in good faith that there is evidence of a crime occurring on the premises of PROVIDER
3. Alerting law enforcement officials to the death of a patient, when there is a suspicion that the death resulted from criminal conduct.
4. Responding to an emergency off premises, which may have been the result of criminal activity
5. Reporting to law enforcement as required by law
6. Compliance with a court order or court-ordered warrant, subpoena or summons issued by a judicial officer
7. Administrative request from law enforcement which must include statements that the information is relevant, material, specific and limited in scope and reasonable assertions that de-identified information cannot be used.
8. In response to protected health information for purposes of identification or location of a suspect, fugitive, material witness or missing person, information must be limited to basic demographic and health information about the patient.
9. Response to a request for protected health information about an adult patient when they agree (limited circumstances when the patient is unable to agree). Child abuse or neglect may be reported without patient consent to any law enforcement official authorized by law to receive such reports.

Disclosure or Inspection of Deceased Person's Personal Health Information

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502(f) and § 164.502 (g)

As a general rule a deceased patient's protected health information is treated the same under the HIPAA Privacy Rule as if the patient were living. PROVIDER would require the authorization of the deceased patient's personal representative or executor before complying with any requests for disclosures as outlined in the **Request for Accounting Disclosures Policy** and **Disclosures to Law Enforcement Policy**.

Disclosures of protected health information for treatment purposes, even for another individual, do not require an authorization; consequently, PROVIDER may disclose a decedent's protected health information to a health care provider treating a surviving relative.

Retention and Disposal Policy of Paper Medical Records

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to disposal and disposition, in accordance with the requirements at § 164.530(c).

PROVIDER is responsible for ensuring the following about medical records.

1. Protected health information retained at a minimum for the specified period, as defined by the Privacy Officer who will take into account all federal, state and HIPAA compliance regulations.
2. Site maintenance of medical records
3. Control of medical records has to be considered when medical records are turned over to Business Associates and authorized legal enforcement entities.

Information must be securely destroyed once that information exceeds its retention period.

Records concerning the destruction of medical records will be maintained indefinitely. Verification of selected disposal processes are necessary.

Breach Notification Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.

PROVIDER and its business associates will provide notification following a breach of protected health information that has been improperly disclosed or used.

PROVIDER is presumed to be in a breach unless demonstrated that there are is a low probability of compromise based on a Breach Risk Analysis addressing the following conditions.

1. The nature of PHI involved, including the type of identifiers and likelihood for re-identification.
2. Who accessed the PHI and to whom was the disclosure made.
3. Whether the PHI actually acquired or viewed.
4. Extent by which risk to PHI has been mitigated.

PROVIDER does have the option to provide notification of a breach following a compromise of PHI without going through the deterministic process of a Breach Risk Analysis.

Following a compromise of protected health information, PROVIDER will provide notification to affected individuals, HHS Secretary, and media in some cases. Employees of PROVIDER should bring PHI related issues to the Privacy Officer.

The Privacy Officer will lead PROVIDER in efforts to remediate the breach. Including addressing any state regulatory compliance concerns regarding the breach, and extra resources needed to property assess the breach internally and externally.

A breach of protected health information as discovered by PROVIDER on the first day that the incident was known or should have been known. The discovery is known is triggered as soon as any employee, officer, or business associate knows or should have known about the breach.

IV. Security Policies

The HIPAA Security Rule and security policies govern electronic protected health information ("ePHI") that is created, used and maintained by **PROVIDER**. Security policy maintains the technical safeguards to ensure confidentiality, integrity and availability ("CIA Triad") of a patient's ePHI.

Security Risk Assessment

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the requirements at § 164.308(a)(1).

There are numerous methods of performing risk assessment and there is no single method or "best practice" that guarantees compliance with the Security Rule.

With that in mind, your process and documentation should include the following elements:

1. The scope of the analysis must take into account all ePHI, regardless of the source or location or the way it is created, received, maintained or transmitted. No matter where or how it exists it must be included in the analysis and documented as such.
2. The locations PHI data is stored, received, maintained or transmitted must be identified and documented.
3. Identify and document reasonably anticipated threats to PHI and vulnerabilities if triggered or exploited by any threat would create a risk of inappropriate access to or disclosure of PHI.
4. Assess and document security measures currently in place to safeguard PHI, defining whether security rule measures required by HIPAA are already in place; and confirm they are configured, monitored and used properly.
5. Document all threat and vulnerability combinations with associated likelihood that may impact confidentiality, availability and integrity of ePHI.
6. Document all potential impacts associated with the exploit of the defined vulnerabilities.
7. Assign risk levels or ratings for all threat and vulnerability combinations.
8. Document a list of corrective actions to be performed to mitigate each risk.

Facility Access Control Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a)(1-2) and 164.530(c).

PROVIDER allows minimum facility access privileges on the basis of how much information is necessary to accomplish work related assignments. Facility access controls protect devices that hold electronic protected health information through the use of

1. proper construction materials and alarms
2. surveillance and intrusion detection mechanisms
3. physical keys, swipe cards, cipher locks, and biometric devices
4. visitor guidelines and escorts
5. protections from natural disasters
6. security guard placement
7. asset identification and enclosures

Device and Media Controls

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).

PROVIDER is committed to appropriate physical safeguards for the storage and destruction of electronic protected health information.

i. Media Disposal

Electronic protected health information on decommissioned devices must be irretrievably destroyed, in order to protect the confidentiality of the data contained.

iv. Media Re-Use

Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.

v. Media Accountability

When using storage devices and removable media to transport EPHI a procedure will be implemented to track and maintain records of the movement of those devices and media and the parties responsible for the device and media during its movement.

vi. Media Storage

All original EPHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that EPHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA’s, when storing original EPHI. Backups of original EPHI must be stored off-site in a physically secure facility.

Final Disposition Policy

It is PROVIDER's policy to hold old computer equipment in inventory when replaced. The older equipment may be stored in a physically secure location and made available for a wide assortment of uses, such as:

1. Older machines are regularly utilized for spare parts.
2. Older machines are used on an emergency replacement basis.
3. Older machines are used for testing new software.
4. Older machines are used as backups for other production equipment.
5. Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
6. Older machines are used to provide a second machine for personnel who often work from home.

At which time older computers are to be finally destroyed, any media containing PHI will adhere to NIST 800-88 standards for acceptable destruction, as follows:
NIST 800-88 "Acceptable Destruction of ePHI":

> For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

Access Control

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).

i. General Access Security

1. Employees will not circumvent established controls and safeguards in place

    - Employees may only access resources through trusted access points and devices
    - Employees must use approved software
    - Employees are prohibited from publishing or making publicly visible any information or details on the internal trusted network.

2. Remote users may only use remote access mechanisms provided by PROVIDER

3. All traffic originating from external sources must go through approved gateways

Users may not extend or retransmit network or application services in anyway. PROVIDER prohibits the use of:

- Routers
- Hubs
- Switches
- Wireless Access Points
- Altering network hardware
- Altering software

4. All systems and devices must comply with relevant Industry and PROVIDER Standards.

5. Employees will be given the access based on the ideas of:

    - Least privilege
    - Separation of duties

ii. Account Management

1. All accounts created must have an associated request and approval.

2. All accounts must be uniquely identifiable

3. Accounts must have passwords which comply with the *Password Policy.*

4. Accounts will be disabled:

    - For extended leave
    - Termination
    - Accounts which have not been accessed as defined by federal, state, or compliance regulations.

iii. Special/Administrative Access Security

1. Specific Scope
    1. Technical Services Administrators
    2. Information Security Administrators
    3. Database Administrators
    4. Property Administrators
    5. Others who may have special access account privileges which are elevated in comparison to everyday users.
2. Users with special/administrative access accounts must have:
    1. Proper training to carry out task
    2. Authorization via established mechanisms
    3. Written acknowledgement of responsibility if user is to have access to sensitive data.
        (1) Written acknowledgement of responsibility if user is to be a custodian of keys to sensitive data.
        (2) Written acknowledgement of responsibility if user has access to the location of keys to sensitive data.
3. Account privileges must be assigned with appropriate authority exercising where appropriate:
    - Least privilege
    - Separation of duties
4. Password
    1. Must adhere to *Password Policy*
    2. Elevated account password must not be the same as:
        - Regular account password
        - Password otherwise used somewhere else
    3. Trusted password escrow for system objects or single administrative systems
5. It is prohibited to grant or enable public/direct access to servers or devices on the internal trusted network

iv. Physical Access Security

1. All physical security systems must comply with regulations
    1.0.1. Building codes
    1.0.2. Fire prevention codes

2. Access to sensitive information or resources must be:

    - Documented
    - Managed

3. Requests for access to resources must come from the system owner

4. Access cards and keys must not be shared or loaned

5. Lost or stolen cards and keys must be reported to appropriate personnel immediately.

    - Access cards and keys must not have any identifying information other than a return mailing address

6. All facilities housing sensitive information, as defined by the *Data Handling and Classification Policy,* will retain:

    - Access logs
    - Visitor logs
    - Logs will be retained for as long as business need or compliance regulations.

7. Access will be revoked upon immediate change in status such as:

    - Privilege change
    - Termination of employment
    - Transfer
    - Termination of contract

v. Vendor Access Security

1. Specific Scope

    - Vendors
    - Contractors

2. Vendor personnel must:

    - Uniquely identifiable
    - Comply with the *Password Policy*
    - Follow all policies as applicable
    - Follow specific change control procedures as applicable
    - Report all security incidents to PROVIDER Information Security

3. Vendor organizations will provide PROVIDER with:

    1. Information systems point of contact for policy compliance

    2. Account representative or manager

    3. A list of employees working on a contract

        (1) Staff changes will dictate the list be updated within 24 hours

    4. Written request for work duties to be performed outside of normal working hours.

4. Vendor maintenance accounts and equipment will be:

    - Disabled until needed and authorized by established procedures
    - Audited when work is completed.

5. Sensitive information will be Surrendered, disposed, or destroyed according to pre-arranged method, with verification to be returned to PROVIDER

Audit Control Policy

It is PROVIDER's policy to ensure that proper implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information ("ePHI").

Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Organization is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Organization will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Information Systems Change Policy

PROVIDER will ensure that the Organization of tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information ("ePHI"). Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Acceptable Use Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).

The purpose of this policy is to outline the acceptable use of computer equipment at PROVIDER. These rules are in place to protect the employee and PROVIDER. Inappropriate use exposes PROVIDER to risks including virus attacks, compromise of network systems and services, and legal issues.

i. Overview

PROVIDER's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to: PROVIDER's established culture of openness, trust and integrity. PROVIDER is committed to protecting our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of PROVIDER. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every PROVIDER employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

vi. General Use and Ownership

1. While PROVIDER's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of PROVIDER. Because of the need to protect PROVIDER's network, management cannot guarantee the confidentiality of information stored on any network device belonging to PROVIDER

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. For security and network maintenance purposes, authorized individuals within PROVIDER may monitor equipment, systems and network traffic at any time.

4. PROVIDER reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

vii. Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private,

corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for WinXP users) when the host will be unattended.

4. Postings by employees from a PROVIDER email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PROVIDER, unless posting is in the course of business duties.

5. All hosts used by the employee that are connected to the PROVIDER Internet/Intranet/Extranet, whether owned by the employee or PROVIDER, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

viii. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., administrative staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of PROVIDER authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PROVIDER-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PROVIDER

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PROVIDER or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any PROVIDER account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to PROVIDER is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, employees to parties outside the company.

16. Making any unauthorized changes, which could directly or indirectly affect the integrity of the computer system or network.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within PROVIDER's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by

PROVIDER or connected via PROVIDER's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Social Media Policy

PROVIDER recognizes that the Internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis.

However, employees' use of social media can pose risks to PROVIDER's confidential, private and proprietary information, reputation and brands, can expose employers to discrimination and harassment claims and can jeopardize the company's compliance with business rules and laws, including but not limited to HIPAA and other privacy laws.

PROVIDER routinely handles confidential protected health information (PHI) of patients, and it is imperative the confidentiality of this information remains secure.

To minimize these business and legal risks, to avoid loss of productivity and distraction from employees' job performance and to ensure that the company's IT resources and communications systems are used appropriately as explained below, PROVIDER expects its employees to adhere to the following guidelines and rules regarding use of social media.

Apart from personal use of social media in accordance with this policy, PROVIDER encourages its employees to participate responsibly in these media as a means of generating interest in PROVIDER's services and creating business opportunities so long as all of PROVIDER rules and guidelines regarding social media usage, particularly in a business context, are adhered to at all times.

i. Compliance with Related Policies and Agreements

All of PROVIDER's other policies that might apply to use of social media remain in full force and effect. Social media should never be used in a way that violates any other PROVIDER policies or employee obligations. If your social media activity would violate any of our policies in another forum, it will also violate them in an online forum. For example, employees are prohibited from using social media to:

- Violate PROVIDER's IT resources and communications systems policies.
- Violate PROVIDER's confidentiality and proprietary rights policies.
- Circumvent PROVIDER's ethics and standards of conduct policies.
- Engage in unlawful harassment.
- Circumvent policies prohibiting unlawful discrimination against current employees or applicants for employment.
- Violate PROVIDER's privacy policies (for example, never access private password-protected sites of co-workers or other PROVIDER stakeholders without permission).
- Violate any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by creating an artificial "buzz" around our business, products or services).

Employees who violate any of the above or other PROVIDER policies may be subject to discipline, up to and including termination of employment.

ix. Personal Use of Social Media

[Personal use of social media is never permitted on working time by means of the company's computers, networks and other IT resources and communications systems.

OR

We recognize that employees might work long hours and occasionally may desire to use social media for personal activities at the office or by means of the company's computers, networks and other IT resources and communications systems. We authorize such occasional use so long as it does not involve vulgar, obscene, threatening, intimidating or harassing content (not otherwise protected or required by law), does not violate any other PROVIDER policies or employee obligations and does not interfere with your employment responsibilities or productivity. Circulating or posting commercial, personal, religious or political solicitations, chain letters, spam or promotion of outside organizations unrelated to company business are also prohibited (unless otherwise protected or required by law).]

x. No Expectation of Privacy

All contents of PROVIDER's IT resources and communications systems are the property of the company. Therefore, employees should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

You are expressly advised that in order to prevent misuse, PROVIDER **reserves the right to monitor, intercept and review, without further notice, every employee's activities using the company's IT resources and communications systems, including but not limited to social media postings and activities, and you consent to such monitoring by your acknowledgment of this policy and your use of such resources and systems.** This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The company also may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Do not use the company's IT resources and communications systems for any matter that you desire to be kept private or confidential from the company.

xi. Business Use of Social Media

If you are required to use social media as part of your job duties, for the company's marketing, public relations, recruitment, corporate communications or other business purposes, you should carefully review PROVIDER's Social Media Business Use Guidelines. Note that PROVIDER owns all social media accounts used on behalf of PROVIDER or otherwise for business purposes, including any and all log-in information, passwords and content associated with each account, such as followers and contacts. PROVIDER owns all such information and content regardless of the employee that opens the account or uses it, and will retain all such information and content regardless of separation of any employee from employment with PROVIDER. If your job duties require you to speak on behalf of the company in a social media environment, you

must still seek approval for such communication from [YOUR MANAGER/DEPARTMENT NAME], who may require you to receive training before you do so and impose certain requirements and restrictions with regard to your activities. Likewise, if you are contacted for comment about PROVIDER for publication, including in any social media outlet, direct the inquiry to [DEPARTMENT NAME] and do not respond without written approval.

xii. Guidelines for Employees' Responsible Use of Social Media

The above material covers specific rules, policies and contractual obligations that employees must follow in using social media, whether for personal or business purposes, in consideration of their employment and subject to discipline for violations. The following sections of the policy provide employees with common-sense guidelines and recommendations for using social media responsibly and safely, in the best interests of PROVIDER. These guidelines reflect the "duty of loyalty" every employee owes its employer, and are intended to add to, not contradict, limit or replace, applicable mandatory rules, policies, legal requirements, legal prohibitions and contractual obligations.

Protect the Company's Goodwill, Brands, and Business Reputation. You are personally responsible for what you communicate in social media. Remember that what you publish might be available to be read by the masses (including the company itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

Make it clear in your social media activity that you are speaking on your own behalf. Write in the first person and use your personal e-mail address when communicating via social media. [Never post anonymously to social media sites when your post could be attributed to PROVIDER, its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders. Anonymous posts can be traced back to the original sender's email address. Follow all guidelines in this policy regarding social media postings.]

If you disclose your affiliation as an employee of PROVIDER, it is recommended that you also include a disclaimer that your views do not represent those of your employer. For example, consider such language as "the views in this posting do not represent the views of my employer." Use good judgment about what you post and remember that anything you say can reflect on PROVIDER, even if you do include a disclaimer. Always strive to be accurate in your communications about PROVIDER and remember that your statements have the potential to result in liability for yourself or the company. PROVIDER encourages professionalism and honesty in social media and other communications.

Respect Intellectual Property and Confidential Information. PROVIDER's [CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT/EMPLOYEE HANDBOOK] restricts employees' use and disclosure of the company's confidential information and intellectual property (see above). Beyond these mandatory restrictions, you should treat the company's trade secrets and other confidential and/or proprietary information and intellectual property accordingly and not do anything to jeopardize them through your use of social media. In addition, you should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for yourself and for PROVIDER.

To protect yourself and the company against liability for copyright or trademark infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate the copyright or trademark of any person or company, ask before making the communication.

Respect and Comply With Terms of Use of All Sites You Visit. Do not expose yourself or PROVIDER to legal risk by using a social media site in violation of its terms of use. Review the terms of use of all social media sites you visit and ensure your use complies with them. If you are using social media as part of your job duties, pay particular attention to terms relating to:

- Prohibitions or restrictions on the use of the social media site, including prohibitions or restrictions on use for advertising, marketing and promotions or other commercial purposes (for example, *Facebook's Statement of Rights and Responsibilities* (its terms of use) and accompanying *Promotional Guidelines* specify the terms for businesses administering promotions through Facebook).
- Ownership of intellectual property used on, or information collected or generated through use of, the site (for example, any of the company's copyrighted material and trademarks that might be posted on the site, or user information the company collects through the site).
- Requirements for licenses or other permissions allowing use by the site owner and other third parties of the company's trademarks or other intellectual property.
- Privacy rights and responsibilities of the site owner and users.

Respect Others. Do not post anything that PROVIDER's patients, clients, customers, business partners, suppliers or vendors would find offensive, including ethnic slurs, sexist comments, discriminatory comments, insults or obscenity.

[Supervisors should refrain from trying to connect with direct reports on social media sites (for example, making friend requests on Facebook). Direct reports may request connections with supervisors, however. Supervisors should not feel pressured to accept the request.

OR

Supervisors and direct reports should refrain from trying to connect with one another on social media sites (for example, making friend requests on Facebook). Neither supervisors nor direct reports should feel pressured to accept any requests from anyone at PROVIDER]

xiii. Conduct not Prohibited by this Policy

[This policy is not intended to preclude or dissuade employees from engaging in legally protected activities/activities protected by state or federal law, including the National Labor Relations Act, such as discussing wages, benefits or terms and conditions of employment, forming, joining or supporting labor unions, bargaining collectively through representatives of their choosing, raising complaints about working conditions for their and their fellow employees' mutual aid or protection or legally required activities.

OR

This policy is not intended to restrict communications or actions protected or required by state or federal law.]

Use of Mobile Device Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, mobile phones, tablets, laptops, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Organization in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Organization networks. Every workstation or server that has been used by either Organization employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Organization data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common practice within the Organization. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of the network. Transportable media received from an external source could potentially pose a threat to the networks. ***Sensitive data*** includes all human resource data, financial data, proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").
Rules governing the use of transportable media include:

1. No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.

2. All USB keys used to store sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.

3. Users must never connect their transportable media to a workstation that is not issued by the Organization.

4. Non-Organization workstations and laptops may not have the same security protection standards required by the PROVIDER, and accordingly virus patterns could potentially be transferred from the device to the media and then back to the workstation.

5. Data may be exchanged between workstations/networks and workstations used within the PROVIDER The very nature of data exchange requires that under certain situations data be exchanged in this manner.

6. Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.

7. When an employee leaves PROVIDER, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

PROVIDER utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all PROVIDER laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

Disaster Recovery Plan

Refer to the organization’s Business Continuity Plan.

V. Reporting Systems, Auditing, and Corrective Action Initiatives

Complaints Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

PROVIDER will investigate all valid complaints in order to ascertain the circumstances surrounding concerns raised by a patient or patient representative regarding privacy.

If patient's rights have been found to have been infringed upon, then PROVIDER will take any and all steps necessary to ensure consistency with HIPAA compliance regulations, state law and internal policies and procedures.

PROVIDER will ensure that every patient will received the highest care and that a compliant will no way inhibit the level of service administered to the patient.

Anti-Intimidation and Anti-Retaliation Policy

PROVIDER must comply with HIPAA and the HIPAA implementing regulations concerning prohibiting intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA in accordance with the requirements at § 164.530(g).

PROVIDER will not intimidate, coerce, discriminate against, threaten or take retaliatory action against an individual for the following reasons.

1. Exercising rights guaranteed under HIPAA
2. Filing of a HIPAA complaint with the Secretary of Health and Human Services.
3. Testifying, assisting or participating in a HIPAA investigation, compliance, review or hearing

PROVIDER will never require employees, officers, contractors or business associates to waive their rights under HIPAA.

VI. Employee Training

NOTE: (MF) Employee Training accounting probably should be kept as a different chart of accounts.

The HIPAAComplete online software system has a full history of all the yearly HIPAA training based on viewing of an online video and required quiz.

Appendix A: Recurring Tasklets

A-1. Privacy Officer – Continuing Education Log

Privacy Officer Name: _____

Continuing Education:

Event Name	Date Attended

A-2. Security Officer – Continuing Education Log

Security Officer Name: _____

Continuing Education:

Event Name	Date Attended

A-3. Documentation of Stakeholders

Company Ownership:

Name	*Title*	*Email Address*	*Phone*

HIPAA Compliance Committee:

Name	*Title*	*Email Address*	*Phone*

A-4. **AUTHORIZATION FOR RELEASE OF INDIVIDUALLY IDENTIFIED HEALTH INFORMATION**

Patient name: _____ **Record Number**: _____

I, or my personal representative, hereby authorize PROVIDER to use or disclose protected health information regarding my care and treatment. I understand that:

1. Information relating to **ALCOHOL/DRUG ABUSE**, **MENTAL HEALTH TREATMENT**, **GENETIC TESTING**, and/or **CONFIDENTIAL HIV-RELATED INFORMATION** will not be disclosed unless I specifically authorize such disclosure by placing my initials in the appropriate space(s) in Item 8(b).

2. Information that is disclosed pursuant to this authorization may be re-disclosed by the recipient and no longer protected by federal or state law. If I am authorizing the disclosure of HIV-related information, the recipient is prohibited from re-disclosing the information without my authorization, unless permitted to do so under state or federal law. I have a right to request a list of people who may receive or use my HIV-related information without authorization.

3. I have the right to revoke this authorization at any time by providing a written notice of revocation to the provider at the address listed below, except to the extent PROVIDER has already relied upon this authorization.

4. Signing this authorization is voluntary. PROVIDER may not condition treatment, payment, enrollment in a health plan or eligibility for benefits on my signing or refusal to sign this authorization, except in limited circumstances.

5. Provider releasing this information (one provider per form)**:**

Name: _____
Address: _____
_____

6. Purpose for release of information:
□ At my request □ Continuity of Care
□ Other:_____

7. Person(s) receiving this information:
□ Send to Name: _____
Address: _____
□ I will pick it up
□ My personal representative _____ will pick it up. (identification required for pick-up)

8. Description of information being released:
(a) Specific date(s) of service (required; list all dates):_____
_____

I would like (choose one)**:**
□ An abstract (pertinent information related to the above listed date(s))
□ My entire Medical Record
□ Other: _____

(b) Include information relating to (initial beside each applicable category):
□ **Alcohol/Drug Treatment** _____ □ **Mental Health Treatment** _____
□ **Genetic Testing Information** _____
□ **Psychotherapy Notes** _____ (If yes, complete a separate authorization form for this purpose)
□ **HIV-related Information** _____ (If yes, complete an official release form)

9. Date or event on which this authorization will end:
□ One-Time Request □ Specific Event or Date: _____

10. Signature: By signing below I acknowledge that I have read and agree with all of the above.
Signature:_____ Date: _____/_____/_____
Print name of patient or personal representative: _____
Personal representative's authority (supporting documentation required):
□Parent □ Guardian □Health Care Agent □ Administrator/Executor
□ Other: _____

THE PATIENT OR PERSONAL REPRESENTATIVE MUST BE PROVIDED WITH A COPY OF THIS FORM UPON SIGNING

Appendix B: Business Associates