0

Heiden Chiropractic Inc.

HIPAA SECURITY AND PRIVACY POLICIES AND PROCEDURES

Prepared by Whyte Hirschboeck Dudek S.C.

Privileged and Confidential

Contents

PURPOSE

The purpose of these policies, procedures and forms is to help ("*Heiden Chiropractic Inc.*") comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the provisions in Subtitle D, Section 13401 of the HITECH Act, signed into law on February 17, 2009 (the "HITECH Act"). Specifically, these laws require *Heiden Chiropractic Inc.* to create and implement policies and procedures related to administrative, physical and technical safeguards, pursuant to the regulations for HIPAA, found at 45 CFR §§ 164.308, 310, 312 and 316 (the "HIPAA Security Rule"), as well as the HIPAA Privacy Rule, found at 45 CFR, Part 164, subpart E.

Every part of the HIPAA Security Regulations is defined as "addressable" or "required." If an implementation specification is described as "required," the specification must be implemented. If a section is specified as "addressable," a covered entity must either implement the specification as listed, implement an alternative measure to accomplish the same purpose, or not implement the specification or an alternative. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. No matter which option is selected, the covered entity's choice must be documented, and should include the factors considered as well as the results of the risk assessment on which the decision was based.

Heiden Chiropractic Inc.'s Security Policies and Procedures will be operated in conjunction with the Security Policies and Procedures adopted by *Heiden Chiropractic Inc.*'s Electronic Medical Record Vendor, attached hereto.

DEFINITIONS

Terms used in these policies and procedures that are specifically defined in HIPAA shall have the same meaning as set forth in HIPAA, HITECH and any other subsequent amendments. A change to these laws which modifies any defined term, or which alters the regulatory citation for the definition shall be deemed incorporated into these policies and procedures.

"Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the protected health information. *See* 45 CFR § 164.402.

"Business Associate" shall mean an entity or person that meets the definition provided in 45 CFR § 160.103, including entities or persons who perform or assist in the performance of functions or activities involving the use or disclosure of individually identifiable health information or provides, other than in the capacity of a member of the workforce of a Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for a Covered Entity.

"Covered Entity" shall mean a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. *See* 45 CFR § 164.103.

"Data Aggregation" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 164.501.

"Designated Record Set" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR §164.501.

"DHHS" means the federal Department of Health and Human Services.

"Electronic Protected Health Information" and/or **"EPHI"** shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, and shall include, without limitation, any EPHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 CFR. Parts 160-164).

"HITECH" means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

"Individual" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103. It shall also include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, and Security Standards for the Protection of Electronic Protected Health

Information (the "Security Rule"), that are codified at 45 CFR parts 160 and 164, Subparts A, C, and E and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

"Protected Health Information" and/or **"PHI"** shall have the meaning given to the term under the Privacy Rule, including but not limited to, 45 CFR § 164.103, and shall include, without limitation, any PHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.

"Required By Law" shall have the meaning given to the term under the Privacy Rule, including but not limited to, 45 CFR § 164.103, and any additional requirements created under HITECH.

"Secretary" shall mean the Secretary of the Department of Health and Human Services or her designee.

"Secured PHI" shall mean PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals, as defined by the Secretary pursuant to 45 CFR § 164.402. As of August, 2009, "Secured Protected Health Information" means PHI that has been encrypted or destroyed. *See* Guidance by DHHS, issued on August 24, 2009, 74 Fed. Reg. 42740. 42742. EPHI has been encrypted if it uses an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. *Id.* Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, available at http://www.csrc.nist.gov/. *Id.* Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. *Id.* These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated. *Id.* Available at http://www.csrc.nist.gov/. As for PHI destruction, paper, film, or other hard copy media should be shredded or destroyed so that the PHI cannot be read or otherwise reconstructed. *See* Guidance by DHHS, issued on August 24, 2009, 74 Fed. Reg. 42740, 42743. For electronic media, destruction includes clearing, purging or destroying consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. *Id.* This guidance may change. It is *Heiden Chiropractic Inc.*'s intent to implement whatever guidance DHHS issues so it may fall within the safe harbor of "secured PHI." The HITECH Act § 13402(h).

"Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 CFR § 164.304.

"Services Agreement" shall mean the underlying agreement(s) that outline the terms of the services that Business Associate agrees to provide to Covered Entity and that fall within the functions, activities or services described in the definition of "Business Associate" at 45 CFR § 160.103.

"Subcontractor" shall mean any vendor or agent of Business Associate that performs services involving the receipt, maintenance, use, transmission, disclosure, and/or creation of PHI on behalf of Business Associate.

"Unsecured PHI" shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section § 13402 of HITECH. 45 CFR § 164.402.

HIPAA SECURITY POLICIES AND PROCEDURES

1. Employee Use of EPHI

It is the policy of *Heiden Chiropractic Inc.* that all employees use workstations in secure manner, particularly when using PHI. *Heiden Chiropractic Inc.* implements and monitors policies and procedures that will, as appropriate, provide or restrict employee access to EPHI and ensure that all members of its workforce have appropriate access to EPHI and prevent unauthorized employees from obtaining access to EPHI. [1]

Accordingly, *Heiden Chiropractic Inc.* has adopted the procedures below:

a. Login procedure[2]

1. The log-in procedure is as follows:

a. Each employee must use their assigned unique user identification to access EPHI.

b. *[Insert #]* failed log-in requests will lock out account;

c. User must contact IT support to get account unlocked;

d. IT support will verify with Security Officer that it is a valid request.

b. Password management[3,4]

Heiden Chiropractic Inc. shall, through its Security Officer, develop, implement and monitor policies and procedures for creating, altering and protecting passwords designed to regulate and monitor access to *Heiden Chiropractic Inc.*'s EPHI.

Heiden Chiropractic Inc.'s Security Officer will be responsible for determining and maintaining documentation reflecting the process and procedures that are reasonable and appropriate for these purposes. Password management procedures shall include:

1. The assignment of a unique password with a minimum of 8 characters, 1 upper, 1 lower, 1 number, 1 symbol, to each person with authorized access which will provide authorized access to the type and extent of EPHI that should be accessible to given individual.

[1] *See* 45 C.F.R. § 164.308(a)(3)(i). Required.
[2] *See* 45 C.F.R. § 164.308(a)(5)(ii)(C). Addressable.
[3] *See* 45 C.F.R. § 164.308(a)(5)(ii)(D). Addressable.
[4] *See* 45 C.F.R. § 164.312(a)(1). Required.

2. Each password will expire every ____ days and employees will be prohibited from using the previous three passwords. All passwords must be changed every ___days.

3. *Password rules*: Passwords must be maintained in a secure manner by the user. *Heiden Chiropractic Inc.*'s Password Policy and Procedure is as follows:

    a. No duplicative or shared passwords.

    b. No displaying of passwords where others can easily view them.

    c. No discussing passwords with others.

    d. Never using the "remember password" feature.

    e. Deleting passwords upon termination of user access.

    f. Immediately reporting all compromised passwords to the Security Officer.

    g. Terminating or replacing passwords that are identified as compromised within one (1) business day.

    h. Password use will be required for access by all remote users.

    i. *Heiden Chiropractic Inc.* 's Security Officer or his or her designee will be responsible for training all users in relation to password use and management.

4. *Time Periods for Access*: Authorized users will be automatically closed out if inactivity on the system occurs for a period of *[Insert #]* minutes or more. Re-access will require use of the unique user identification.[5]

5. Users who violate this policy may be subject to immediate disciplinary action.

6. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for documenting all activities relating to password management. The documentation will be maintained and retained for a minimum of six (6) years from the date of creation.

[5] *See* 45 C.F.R. § 164.312(a)(2)(iii). Addressable.

c. Workstation use [6]

1. User Responsibilities

a. Users will attend a Security Awareness and Training Program and will document attendance at the training program.

b. Users will be trained in relation to workstation use and sign a statement of understanding relating to requirements set forth in HIPAA's Security Rule, an agreement to abide by the security requirements and an agreement to protect the confidentiality of EPHI. The agreement to abide by the security requirements includes an obligation to use workstations appropriately.

2. *Heiden Chiropractic Inc.* Security Officer Responsibilities

a. *Heiden Chiropractic Inc.*'s Security Officer will maintain an accurate inventory of workstations, their location and their supervision.

b. *Heiden Chiropractic Inc.*'s Security Officer or other designated person will be responsible for regulating access to workstations and will monitor the policies and procedures designed to supervise employees. The Security Officer will also be required to train employees on workstation use as it relates to protected health information security.

c. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for monitoring and maintaining compliance with software licensing and copyright laws.

d. *Heiden Chiropractic Inc.*'s Security Officer will ensure that the server has surge protection and a backup power supply. In order to protect *Heiden Chiropractic Inc.*'s EPHI, no eating or drinking will be allowed near the workstations.

e. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for implementing any reasonable methods for maintaining the integrity of EPHI, including the use of anti-virus software to be updated as needed to protect the integrity of EPHI. A password control system will be installed or implemented on each workstation and access will only be provided to authorized users, who will be monitored by the Security Officer.

[6] *See* 45 C.F.R. § 164.310(b) and (c). Required.

f. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for monitoring and tracking users of EPHI, and employees may not conceal their identity when accessing or modifying EPHI.

g. Employees are responsible for all information and data entered into or transmitted from *Heiden Chiropractic Inc.*'s system.

h. Each workstation will have backup procedures that will comply with the *Data Backup Plan*. Backup procedures will be performed regularly.

i. Each user must log-off when away from his/her workstation for more than five minutes; the Security Officer can make exceptions to this procedure. The log-off procedure requires users to hit (Ctrl+Alt+Delete) and select "log-off."

j. Monitors will be located in secure locations and will be positioned in a manner as to avoid unauthorized access or viewing by other employees or visitors to *Heiden Chiropractic Inc.* In. Privacy screens will be used when necessary and appropriate. Rooms that house workstations with EPHI should be locked during non-business hours whenever possible.

k. Printing of EPHI will only occur as needed by authorized users and must comply with procedures developed by *Heiden Chiropractic Inc.*'s Security Officer. Incoming faxes will arrive via a fax machine that is housed in a secure area, away from public or easily accessible areas. All hard copy printouts and faxes of EPHI will be removed from the machine immediately.

l. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for documentation, maintenance and retention of all information relating to workstation use. The information will be retained for at least six (6) years from the date of creation.

3. Prohibited Workstation Practices

a. The use of programs or connections to the Internet that may affect confidentiality, integrity or availability of EPHI.

b. Downloading or installing unapproved programs or applications.

c. Unauthorized access to any workstation.

d. Unauthorized use, dissemination or access to EPHI.

e. Refusal to abide by the security requirements of *Heiden Chiropractic Inc.*.

f. Employees may not access any confidential protected health information without proper access. Furthermore, no data should be downloaded from *Heiden Chiropractic Inc.*'s system without prior authorization from the Security Officer.

2. Authorization of Access to EPHI

Heiden Chiropractic Inc.'s Security Officer will be responsible for procedures that define levels of access (categories) for all authorized users and establish and modify access. The procedures will incorporate the current "best practices," and any applicable standards issued by DHHS, in access control that are deemed reasonable for *Heiden Chiropractic Inc.*. The procedures regulating authorization of access, to the extent reasonable and appropriate, should result in access being reviewable and controllable.

To authorize and/or supervise employees who work with EPHI or in locations where it might be accessed, *Heiden Chiropractic Inc.* follows this procedure:[7]

a. Authorization[8]

1. *Heiden Chiropractic Inc.*'s Security Officer will identify and document, on the *Workforce Access Determination Form*, the person or classes of persons comprising the workforce within the healthcare facility.[9] The workforce classifications may include:

a. Personnel who handle protected health information directly, such as clinicians, data entry, data analysis or claims processing personnel.

b. Personnel who handle protected health information indirectly, such as information technology employees.

2. *Heiden Chiropractic Inc.*'s Security Officer will identify the category or categories of protected health information. The categories may include:

a. *Highly confidential information*: includes healthcare information that relates directly to the health of the patient.

b. *Moderately confidential information*: includes healthcare information such as past history or identification of family members.

c. *Less confidential information*: includes healthcare information that is not directly related to the health of the patient such as

[7] *See* 45 C.F.R. § 164.308(a)(3)(ii)(A). Addressable.
[8] See 45 C.F.R. § 164.308(a)(4). Required.
[9] *See* 45 C.F.R. § 164.308(a)(4)(ii)(B). Addressable.

demographic information or insurance information. This information may also be information that may be disclosed without a patient authorization.

3. *Heiden Chiropractic Inc.*'s Security Officer will identify each person who needs access to categories of EPHI and, in order to comply with the Minimum Necessary standard, will grant access only to those categories that are necessary. See *Workforce Access Determination Form*. *Heiden Chiropractic Inc.*'s HIPAA Security Officer will then develop access rules to control the levels of access to EPHI by employees.

4. *Heiden Chiropractic Inc.*'s Security Officer will authorize access and supervise workforce access to EPHI. *Heiden Chiropractic Inc.*'s Security Officer may delegate authorization of access and supervision of access to supervisory personnel.

5. *Heiden Chiropractic Inc.*'s Security Officer will implement appropriate training relating to access including personal and professional responsibilities relating to access and sanctions for inappropriate access.

6. *Heiden Chiropractic Inc.*'s Security Officer will be provided access to EPHI as is necessary to implement and monitor workforce access.

7. Procedures for auditing access will be deemed a critical element of the access control process.

8. *Heiden Chiropractic Inc.*'s Security Officer will retain all documents and forms to document access, authorization, supervision and compliance with the state and federal security requirements. Information relating to access will be retained for a minimum of six (6) years from the date of creation.

b. Employee Access

To determine whether access of an employee to EPHI is appropriate, *Heiden Chiropractic Inc.* follows this procedure:[10]

1. *Background Verification Actions*. In accordance with the Fair Credit Reporting Act ("FCRA"), any general background investigation will be conducted with the full knowledge and permission of the candidate or employee who is the subject of an investigation and *Heiden Chiropractic Inc.* will ask the individual to sign a release which complies with the FCRA requirements. See *Pre-Employment Authorization Form*.

    a. *Heiden Chiropractic Inc.* will conduct background investigations, including credit reports, on all persons to be employed by *Heiden*

[10] *See* 45 C.F.R. § 164.308(a)(3)(ii)(B). Addressable.

Chiropractic Inc. in positions that involve access to financial or personal information of patients. Results of such investigations shall be kept in a restricted access file by the Security Officer and not in the general personnel or employee file.

2. *Retention of Workforce Clearance Results*. All workforce clearance processes will be documented by the Security Officer. Workforce clearance documentation and supporting information will be available to only the Security Officer, and he/she will maintain such information in a restricted access file in the Security Officer's office available only to him/her. All workforce clearance results are considered confidential. This information will be retained for a minimum of six (6) years from the date of its creation or the date when it was last in effect.

3. *Re-checks in Connection with Workforce Clearance Procedures*. The workforce clearance process will be initiated when deemed appropriate by *Heiden Chiropractic Inc.*'s Security Officer or in response to environmental or operational changes affecting the security of *Heiden Chiropractic Inc.*'s EPHI.

4. *Heiden Chiropractic Inc.*'s Security Officer will establish access privileges utilizing job titles and categories as outlined in the *Workforce Access Determination Form* and communicate those privileges to the IT consultant. Establishment of access may be initiated by written requests relating to a new employee or a change in employee status and/or written requests based on an employee's need to access EPHI.[11]

5. Once access is granted to an employee, *Heiden Chiropractic Inc.*'s Security Officer will ask the IT consultant to assign a unique user identification and/or password, in accordance with *Heiden Chiropractic Inc.*'s Unique User Identification Policy and Procedures.

6. All activities relating to establishing and modifying access will be documented and retained by the Security Officer for at least six (6) years from the date of creation.

3. EPHI Use

a. Transmission

Heiden Chiropractic Inc. shall, through its Security Officer, implement appropriate technical security measures – including integrity controls and encryption mechanisms, to the extent reasonably possible – to protect against unauthorized access and/or modification to electronic protected health

[11] *See* 45 C.F.R. § 164.308(a)(4)(ii)(C). Addressable.

information ("EPHI") being transmitted over an electronic communications network and shall prevent the inaccurate transmission of information over *Heiden Chiropractic Inc.*'s networks. [12,13]

1. When the network architecture, protocol, hardware and management are not sufficient to secure EPHI during transmission over an electronic network outside of *Heiden Chiropractic Inc.*, the transmission must either:

    a. Implement an encryption mechanism between the sending and receiving entities; or

    b. The file, document or folder containing EPHI must be encrypted before transmission.

2. The following measures may be considered:

    a. Assurance of integrity by network configuration, which can include encryption if integrity cannot be assured by the network configuration.

    b. Use of a digital signature.

3. If determined necessary by the Security Officer when transmitting EPHI using movable media, including floppy disks, CD ROM, memory cards, magnetic tape, removable hard drives, or mobile drives such as smart phones or tablets, the file, document or folder containing the EPHI must be encrypted.

4. When transmitting EPHI over an electronic network within *Heiden Chiropractic Inc.*, the EPHI is password protected before transmission.

5. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for documenting all activities related to technical security measures relating to integrity controls and the transmission of EPHI and maintain and retain such documentation for at least six (6) years from the date of creation.

b. Authentication[14,15]

1. **To the extent possible,** *Heiden Chiropractic Inc.* shall, through its Security Officer, implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

[12] *See* 45 C.F.R. § 164.312(e)(1). Required.
[13] *See* 45 C.F.R. § 164.312 (e)(2)(i-ii). Addressable.

[14] *See* 45 C.F.R. § 164.312(c)(1). Required.
[15] *See* 45 C.F.R. § 164.312(c)(2). Addressable.

Reasonable mechanisms shall be implemented to ensure data accuracy when it is transferred between computers or read from electronic media.

a. *Heiden Chiropractic Inc.* shall, through its Security Officer, implement policies and procedures to protect EPHI from improper alteration or destruction, including mechanisms to authenticate EPHI that has not been properly altered or destroyed.

b. To ensure data integrity,[16] *Heiden Chiropractic Inc.* may use a review process by another employee and/or an application or program to ensure data integrity. Intrusion detection systems and audit trails to prevent unauthorized access may also be useful, and backup systems to prevent data loss may be necessary. Other reasonable methods may include implementation of integrity controls, interface programs, software products (including antivirus software) and protecting media from exposure to excessive heat or magnetic fields.

c. *Heiden Chiropractic Inc.*'s Security Officer will document all data integrity implementation activities and maintain and retain that documentation for a period of at least six (6) years from the date of creation.

2. User authentication[17]

Heiden Chiropractic Inc. shall, through its Security Officer, implement procedures to verify the identity of persons or entities[18] seeking access to EPHI. Authentication[19] procedures may include the following:

a. All employees with authorized access to the network, system or application that contains EPHI must satisfy a user authentication mechanism that includes unique user passwords.

b. Employees with authorized access to any network, system or application are not allowed to misrepresent themselves by using another person's user identification and password, smart card, or other access control[20] mechanism.

[16] "Integrity" means the property that data or information has not been altered or destroyed in an unauthorized manner. Among other things, data integrity can be lost by human intervention, hacking, data input errors, and malicious software. 45 CFR § 164.304.
[17] *See* 45 C.F.R. 164.312(d). Required.
[18] "Entity" means an organization or computer system. "Individual" means a person.
[19] "Authentication" means the verification of the identity of a user or other entity as a prerequisite to allowing access to information systems. *See* 45 CFR § 164.304.
[20] "Access Control" means the prevention of access to EPHI by unauthorized individuals.

c. All employees will make reasonable efforts to verify the authenticity of the receiving person or entity prior to transmitting EPHI.

d. Non-compliance with this policy may result in immediate employee disciplinary action.

e. *Heiden Chiropractic Inc.*'s Security Officer will document all activity related to verification of authenticity and maintain all such documentation for a minimum of six (6) years from the date of creation.

c. Audit Controls[21]

1. *Heiden Chiropractic Inc.* shall, through its Security Officer and IT consultant, implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI and provide evidence of identified system activities and an audit trail of activities performed.[22]

2. *Heiden Chiropractic Inc.*'s Security Officer will evaluate current hardware and software to determine whether they contain the capability to record and examine activity in the information system.

3. The audit trails will be accessible to the Security Officer and, when possible, stored on a separate computer system to maintain their confidentiality.

4. *Heiden Chiropractic Inc.*'s Security Officer will notify employees that their activities are monitored by an audit trail. The audit trail should provide the Security Officer with a chronological trail of computer events that gives information about an operating system, an application or user access. The audit trail will be used to monitor computer activity to assist in determining:

a. Whether a security incident has occurred.

b. Whether there is an indication of unauthorized access.

c. Whether there is unusual employee access.

d. Whether there is unusual activity that requires further investigation.

[21] *See* 45 C.F.R. § 164.312(b)(1). Required.
[22] Audit Controls are the technical mechanisms that track and record computer activities. 45 CFR § 164.132(b)(1).

5. Various activities can be identified by using audit control logs. Such activities include: users accessing more information than they are authorized to access, prolonged log-in or failure to log-out, password sharing, unusual log-in activity, inappropriate access for a particular user, internet use of a user, user downloading, and use of harmful programs that interfere with the system's efficiency.

6. *Heiden Chiropractic Inc.*'s Security Officer will review the records of system activities and document the mechanisms that record and examine activity in the information systems. The documentation will be maintained by the Security Officer for a minimum of six (6) years from the date of creation.

4. Employee Training, Discipline, and Termination

a. Security training[23] will be based on employee's job responsibilities, and will be applicable to the employee's daily tasks. The importance of security responsibility will be included on each employee's job description.

1. Security training will be delivered to all employees during initial orientation, and thereafter, at least annually, and will include at minimum, information regarding the following topics:

a. Overall discussion of threats and vulnerabilities specific to EPHI;

b. Information access control;

c. Personnel clearance levels;

d. Incident reporting;

e. Viruses and other forms of malicious software;

f. User log-in monitoring;

g. Password maintenance;

h. Social engineering;

i. Security principles; and

j. HIPAA and organizational privacy and security rules, as amended from time to time, *Heiden Chiropractic Inc.*'s policies and procedures, and the sanctions, and civil and criminal penalties prescribed for wrongful actions.

[23] *See* 45 C.F.R. § 164.308(a)(5)(i). Required.

2. Information access control education will include, at least, access limitations to control and regulate employee access to information.

3. Personnel clearance level education will include, at least, clearance level limitations, including controls for regulating access to information based on such clearance levels.

4. Incident reporting education will include, at a minimum, warning signs of an incident and persons to notify when an incident is suspected. Furthermore, incident reporting education will emphasize that an incident should be disclosed to only those individuals with a need-to-know. Incident reporting education will also include any steps necessary to contain the incident.

5. Virus protection (malicious code) education will include, at a minimum, education of potential harm that can be caused by viruses, how to prevent viruses, and procedures to follow when a virus is detected.

6. User log-in education will include, at a minimum, configuration of components to record log-in attempts (both successful and unsuccessful), as well as automated lockout and reporting after [*Insert #*] failed attempts. User log-in education will also stress both (i) the importance of monitoring log-in success or failure and the steps necessary to check log-in information and report any suspicious information or activity and (ii) the user's responsibility to ensure the security of health care information.

7. Password management education will include, at a minimum, rules to be followed in creating and changing passwords, as well as emphasis on the importance of keeping passwords confidential.

8. Social engineering education will include, at a minimum, emphasis on (i) adhering first to all published policies and procedures, despite claims by persons that they should do otherwise, (ii) the practice of verifying an official's identity, position, and/or authority prior to taking direction from that person with respect to security measures, and (iii) a sampling of common "social engineering" measures and countermeasures.

9. Standards, policies and procedures will include, at a minimum, an overview of (i) the HIPAA security standard, and (ii) the policies and procedures, including how to access and gain clarification regarding such policies and procedures. Discussion of sanctions and other penalties will also be discussed in the standards, policies, and procedures.

10. *Heiden Chiropractic Inc.* will issue periodic reminders and security updates,[24] as deemed necessary by *Heiden Chiropractic Inc.*'s Security Officer, to include topics such as password security, malicious software, incident identification and response, access control, and last log-in monitoring.

b. It is the policy of *Heiden Chiropractic Inc.* to enforce the protection of EPHI in a consistent manner; however, no single set of disciplinary options may be appropriate in every single case. Therefore, *Heiden Chiropractic Inc.* retains the discretion to structure disciplinary sanctions as the circumstances warrant. There are certain offenses and violations so serious that immediate dismissal may be appropriate. When an employee is determined to have engaged in a security violation, he/she may be subject to discipline under this policy, up to and including discharge. *Heiden Chiropractic Inc.* will invoke discipline or sanction procedures in a reasonable and consistent fashion

1. *Heiden Chiropractic Inc.* shall implement the following procedures:

a. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for identification, investigation and responding to suspected or known security incidents. *Heiden Chiropractic Inc.*'s Security Officer will also be responsible for mitigation and documentation of security incidents and their outcomes, including following the Notice of Breach procedure.

b. *Heiden Chiropractic Inc.* will appropriately discipline and sanction employees and employees for any violation of state and/or federal security laws or of *Heiden Chiropractic Inc.*'s privacy or security policies and procedures.

c. Each employee will sign a confidentiality statement that acknowledges his/her understanding of the requirements set forth in state and federal requirements relating to privacy and security of EPHI. The confidentiality statement will also acknowledge that violations of privacy or security may lead to disciplinary action.

d. If the Security Officer has determined that a security violation has occurred, appropriate sanctions will be applied to the employee(s).

e. *Heiden Chiropractic Inc.*'s Security Officer will mitigate any identified security violations, as appropriate, and in a timely manner.

f. *Heiden Chiropractic Inc.* shall not retaliate against any employee or individual that reports a security violation or incident.

[24] *See* 45 C.F.R. § 164.308(a)(5)(ii)(A). Addressable.

g. Sanctions against employees that do not comply with or violate security policies or procedures will be commensurate with the gravity of the violation and may include re-training, verbal and written warnings, suspension or termination.

c. *Heiden Chiropractic Inc.* will terminate employee access to EPHI as appropriate. This determination may be made for a variety of reasons, such as termination of employment, a workforce clearance process that indicates an individual may not be authorized access, or an employment sanction process. *Heiden Chiropractic Inc.*'s Security Officer will document when access by an employee has been terminated. See *Termination of Access Form*

1. When possible, the access termination process will include the following:

   a. An interview process that clearly explains to the employee that his/her access, supervised or unsupervised, to EPHI has been terminated and is now denied.

   b. The employee will be informed that unauthorized access may result in civil and/or criminal penalties.

   c. The employee will sign a document indicating that he/she understands that access has been terminated and unauthorized access may result in civil or criminal penalties. See *Termination of Access Form.*

2. When an employee's access is terminated, the Security Officer or his or her designee will terminate all access processes implemented by that employee. This process will include:

   a. Disabling the user account in the Active Directory.

   b. The employee's log-in, password, or other access method(s) will be terminated or invalidated.

   c. Any mechanical access devices and any other relevant physical access or mobile devices, such as keys, swipe cards or company-owned smart phones or tablets, will be returned to the Security Officer.

   d. *Heiden Chiropractic Inc.* will determine who is to have mail/data access to terminated employee's information.

   e. All remaining employees will be required to change their passwords.

   f. The IT support staff will change the VPN password.

3. *Heiden Chiropractic Inc.*'s Security Officer will document termination of access processes. The documentation will be retained by the Security Officer for a minimum of six (6) years from the date of creation.

4. The following are examples of the types of disciplinary actions that may be taken in response to an intentional or an inadvertent violation of the *Heiden Chiropractic Inc.*'s security policies and procedures and can be included by *Heiden Chiropractic Inc.* in the Sanctions Procedures discussed above.

    a. Verbal or written warning or reprimand, documented in file.

    b. Removal of system privileges or placement in a position without duties involving EPHI.

    c. Some type of performance coaching plan or mentoring.

    d. Re-education or re-training.

    e. Suspension with or without pay.

    f. Recalculation and forfeiture of past clinical compensation based on non-complaint activity.

    g. Dismissal or termination.

    h. Notification that a security violation may be reported to law enforcement personnel, regulatory or licensing personnel or other appropriate sources and may result in civil or criminal penalties or prosecution.

5. All employees of *Heiden Chiropractic Inc.* should be aware that there are a number of factors considered when determining the seriousness of a violation and the appropriate discipline. Any decision to impose discipline will be carefully documented with reference to specific factors that justify the discipline imposed. The following are examples of various "aggravating factors" that may increase the seriousness of a violation, and as a result, the severity of the discipline imposed:

    a. The violation occurred after a previous disciplinary action for another violation.

    b. The violator deliberately avoided or failed to check whether a particular course of action was prohibited and/or the violation was committed knowingly.

    c. The suspected violator attempted to conceal his/her violation, lied and/or was dishonest during the investigation.

d. There was a pattern of misconduct.

e. The violation involved retaliation against other persons who reported violations of the law or the Compliance Plan in good faith.

f. Serious damage to *Heiden Chiropractic Inc.*'s reputation or financial condition was caused by the violation.

g. The violator was a member of management.

h. The violation was criminal in nature.

6. Alternatively, the following list contains various "mitigating factors" that may work to decrease the seriousness of a violation and, consequently, the severity of the discipline imposed:

a. The suspected violator voluntarily reported the violation and/or cooperated with investigation of the violation.

b. The violation was not undertaken for personal benefit.

c. The suspected violator's role in the violation was minor or incidental.

7. If a violation of the law or security policies and procedures has occurred, a disciplinary report should be prepared summarizing the violation and discipline imposed. The disciplinary report should be included in the employee's personnel file. Furthermore, a copy of the disciplinary report should be forwarded to the Security Officer. All documentation will be maintained by the Security Officer for at least six (6) years from the date of creation.

5. EPHI Breaches

Heiden Chiropractic Inc. implements and monitors policies and procedures to prevent, detect, contain and correct security violations.

a. Preventing breaches[25,26]

1. *Heiden Chiropractic Inc.*'s security management process will include the following components:

[25] *See* 45 C.F.R. § 164.308(a)(1)(i). Required.
[26] *See* 45 C.F.R. § 164.308(a)(1)(ii)(A). Required.

a. An accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by *Heiden Chiropractic Inc.*. The analysis should:

i) Inventory and identify all information systems that contain or process electronic health care information.

ii) Designate a staff member to report on each area identified in the inventory.

iii) Identify and inventory all security policies, procedures and practices.

iv) Identify all Business Associate Agreements or other arrangements using PHI.

v) Assess compliance levels using the detailed *Risk Analysis Form*.

vi) Using the data gathered by the risk analysis, compile a comprehensive inventory documenting the major components/structure of and threats to *Heiden Chiropractic Inc.*'s electronic information system

b. An annual review and update of the risk analysis to make any necessary adjustments to adapt to technology changes and to maintain compliance with the HIPAA Security Rule.

c. A sanction policy and procedure designed to implement appropriate sanctions against employees who fail to comply with the security policies and procedures of *Heiden Chiropractic Inc.*.

d. Implementation of an information system activity review process that provides regular records review of all information system activity, including audit logs, access tracking reports and security incident notifications.[27]

i) In coordination with the Audit Controls Procedure, identified above, *Heiden Chiropractic Inc.*'s internal audit procedure may implement audit logs, activity reports or other mechanisms to document and manage information system activity.

(A) The processes implemented to provide review will be designed to promote a continuing review of

[27] *See* 45 C.F.R. § 164.308(a)(1)(ii)(D). Required.

information system activity that will assist in the identification of potential and/or actual security breaches so that immediate corrective action may be taken

ii) *Heiden Chiropractic Inc.*'s Security Officer or his or her designee will identify what information or reports are needed by the information system to adequately audit internal electronic security processes.

(A) *Heiden Chiropractic Inc.*'s Security Officer will regularly review the electronic system activity reports

(B) *Heiden Chiropractic Inc.*'s Security Officer will regularly review the electronic system activity reports.

(C) *Heiden Chiropractic Inc.*'s Security Officer or his or her designee, based on a review of this information and system activity reports, will develop parameters for "normal" or "average" activity levels. Normals may be based on access at a specific site, frequency of access or other relevant criteria.

(D) Based on development of "normal" information system levels, the Security Officer will investigate identified abnormalities or unusual information system activities. Investigation may include interviewing employee(s), reviewing system activity information, and/or any other additional information gathering that may be necessary.

(E) *Heiden Chiropractic Inc.*'s Security Officer will be responsible for any necessary response to the identified security abnormality. The response may include correction of any information system security problem and/or employee education or sanction.

(F) *Heiden Chiropractic Inc.*'s Security Officer will be responsible for collecting, documenting and maintaining information system activity reports and related activities, including investigation and mitigation. Documentation of information system activity review, investigation and/or resolution will

be maintained by the Security Officer for a minimum of six (6) years from the date the information was created.

b. Security Incident[28]

Heiden Chiropractic Inc. shall, through its Security Officer or his or her designee, develop, implement and monitor policies and procedures in compliance with the HIPAA Security Rule Requirements to (i) investigate, identify and respond to suspected or known security incidents,[29] (ii) mitigate pursuant to the HIPAA Security Rule Requirements, the harmful effects of security incidents that are known to *Heiden Chiropractic Inc.*, and (iii) document security incidents and their outcomes.

1. *Heiden Chiropractic Inc.*'s efforts will include:

   a. *Heiden Chiropractic Inc.*'s Security Officer will investigate any identified security violation. The Security Officer will also try to identify the cause and effect, if any, of the incident and will preserve such information to the extent possible. The investigation process will be documented on the *Investigation of Security Incident Form*

   b. All employees and independent contractors will identify and report any actual, attempted or threatened breach of security of EPHI and the outcome to the Security Officer as soon as possible after the incident has been identified and, at the latest, within 24 hours of identifying the incident, through any appropriate means of communication, as long as such report is clearly transmitted to *Heiden Chiropractic Inc.*'s Security Officer.

      1. No retaliation toward an employee will be permitted or tolerated for reporting of security incidents.

      2. *Heiden Chiropractic Inc.*'s Security Officer will attempt to preserve all evidence of the security incident and will document all security incidents and their outcome either identified by the Security Officer or reported by the workforce or others to the Security Officer in the Security Incident Log. *Heiden Chiropractic Inc.*'s Security Officer will also document any other security issues and outcomes in the Security Incident Log.

[28] *See* 45 C.F.R. § 164.308(a)(6)(i) and (ii). Required.
[29] Security incident means an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with operations in an information system.

c. *Heiden Chiropractic Inc.*'s Security Officer will mitigate against the harmful effects of security incidents according to the Notice of Breach Policy and Procedure.

    1. Mitigation may also include preventing future incidents, notifying the affected individuals, providing assurances to affected individuals, and continuing to monitor incidents to prevent future occurrences.

d. Each incident reported to the Security Officer shall be documented in a manner that memorializes the date(s) of the incident and report, the reporting employee, a description of the incident and related investigation, findings and recommendations for resolution of the incident. See *Security Incident* Reporting *Form*. *Heiden Chiropractic Inc.*'s Security Officer will also document all security incident processes, including security incidents, outcomes, corrective action and mitigation taken in the *Security Incident Log.* The Log will contain documentation of the identified security issue and the individual(s) or department(s) affected. This documentation will be maintained in a confidential manner by the Security Officer for a minimum of six (6) years from the date the documentation was created.

e. Training of all employees and other users in relation to identification, response and reporting of security incidents.

f. *Heiden Chiropractic Inc.*'s Security Officer will implement all necessary precautions to ensure that the documented security incident does not recur.

g. In the event of a security incident, the Security Officer, working in conjunction with the human resources department, will determine the appropriate level of discipline (which may include termination) based on the seriousness of the incident and whether the incident was intentional and/or the result of a pattern or practice. Any disciplinary action taken against an employee will be documented in the employee's file.

h. *Heiden Chiropractic Inc.*'s Security Officer will address all security incidents on a case-by-case basis. Security incidents will be remedied to prevent future incidents. Remedying an incident may include technology changes, procedure updates, workforce training or retraining, and (if necessary) sanctions. If a security breach continues even after *Heiden Chiropractic Inc.* has been made aware of it, the IT consultant will contact the ISP account and pull that account offline. The IT consultant will also deploy a technician for testing and resolution. Any known or intentional

security violations by employees of *Heiden Chiropractic Inc.* will be handled in accordance with the Sanction Policy and Procedures. All responses to security incidents will be documented by *Heiden Chiropractic Inc.*'s Security Officer. [30]

2. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for all enforcement activities related to a security incident.

6. Emergency Access to EPHI

a. Emergency access[31]

1. *Heiden Chiropractic Inc.* shall, through its Security Officer, establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.

2. *Heiden Chiropractic Inc.*'s Security Officer may implement the emergency access procedures when an incident partially or completely disables the central computing functions of *Heiden Chiropractic Inc.*.

3. *Heiden Chiropractic Inc.*'s Security Officer will create a list that specifically identifies the job title, reason for emergency access, date access granted and name of individuals who have been granted emergency access. The list will also include designation and contact information of backup individuals allowed emergency access if the above-referenced, listed individuals are unavailable or unable to function. All individuals authorized to have emergency access will be notified of the authorization and be trained on procedures relating to emergency access.

4. *Heiden Chiropractic Inc.*'s Security Officer will delineate the procedures for emergency access. The procedures are to be implemented in and limited to actual emergencies and will bypass formal access procedures. The procedures may include:

a. Creating a specific user account providing full access to all EPHI (an administrator account).

b. Creating a second password rather than a separate account providing full access.

c. Other technical accessibility methods to allow immediate and full access.

[30] *See* 45 C.F.R. § 164.308(a)(6)(ii). Required.
[31] *See* 45 C.F.R. § 164.312(a)(2)(ii). Required.

5. The emergency access will be tracked and documented based on capabilities of the system. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate, and any inappropriate emergency access will be treated as a security incident.

6. Emergency access will be considered terminated as soon as it is no longer necessary.

7. Inappropriate use of emergency access will be considered a reportable security incident and may subject an individual to immediate disciplinary action.

8. All activities related to emergency access will be documented by the Security Officer. The documentation will be retained and maintained for at least six (6) years from the date of creation.

b. Contingency Plan[32]

Heiden Chiropractic Inc. is committed to maintaining formal practices for responding to emergencies or other occurrences (for example, fires, acts of vandalism, system failures, natural disasters, etc.) (hereinafter, "emergency situation(s)" or "disruptive occurrence(s)") that damage systems containing EPHI and will, through its Security Officer, continually assess potential risks and vulnerabilities to protected health information in its possession, for the purposes of developing, implementing, and maintaining appropriate administrative, physical, and technical security measures so as to enable *Heiden Chiropractic Inc.*'s compliance with 45 CFR § 164.308.

These practices (the "Contingency Plan") apply to all electronically maintained or transmitted health information pertaining to an individual and serves as the master plan for responding to system emergencies, ensuring continuity of operation during an emergency, and recovering from a disaster.

1. All employees shall be trained regarding the Contingency Plan, which will be reviewed and tested in some form at least once every year, and updated and/or amended if necessary.

2. *Data Backup Plan*. Procedures shall be established and implemented to ensure the existence of retrievable exact copies of EPHI.[33]

    a. *Heiden Chiropractic Inc.*'s Security Officer shall identify, based on any criticality analysis performed, as set forth below (specific to data sets) and/or any alternative procedures, the backup methods

[32] 45 CFR § 164.308 (a)(7). Required.
[33] 45 CFR § 164.308(a)(7)(ii)(A). Required.

(e.g., full, incremental, or differential backup) and materials (e.g., CD-ROM, thumb drives, magnetic tape, or floppy disks) to be used, the frequency of performing backups and the person(s) responsible for performing, cataloging, inspecting, storing and securing the backups.

b. Storage and removal of backups shall be monitored to ensure all applicable access controls are enforced. Storage requirements for each backed up data set shall be monitored to ensure records are maintained for the appropriate time period.

c. The procedures and related documentation for Data Backup and recovery will be tested for weakness and revised as needed.

3. *Disaster Recovery Plan*. Procedures shall be established and implemented to facilitate the restoration of data lost as a result of disruptive occurrences.[34]

a. In the event of any data loss, authorized person(s) shall retrieve the latest copy of backed up data from the secure location or, if necessary data set(s) have not been archived, efforts will be made through formal channels, such as retransmission from original sources, to collect the data.

b. In the order of any established pre-determined criticality (especially with regard to the availability of data) or alternative evaluative standards established by *Heiden Chiropractic Inc.*'s Security Officer, these person(s) will load the data to the appropriate components (in accordance with applicable access control policies) and ensure the data restoration was successful.

c. The procedures and related documentation for disaster recovery will be tested for faults and weaknesses and amended accordingly.

4. *Emergency Mode Operation Plan*. Procedures shall be established to enable the continuation of *Heiden Chiropractic Inc.*'s operations following disruptive occurrences.[35]

a. In the event of an emergency, the Security Officer will contact the IT consultant. The IT consultant may make the server image available/loaned hardware. VPN/remote access can be utilized to access data from any internet connection. Relocation of operations to such a remote site will be executed as necessary in the event of an emergency.

[34] 45 CFR § 164.308(a)(7)(ii)(B). Required.
[35] 45 CFR § 164.308(a)(7)(ii)(C). Required.

b. *Heiden Chiropractic Inc.*'s Security Officer or his or her designee shall designate specific roles and responsibilities to initiate and maintain emergency mode operations, including information system and security personnel. Security Officer will follow emergency access control requirements for emergency mode operations and ensure the access control matrices reflect such requirements.

5. *Testing and Revision Procedures*.[36] *Heiden Chiropractic Inc.*'s Security Officer may implement procedures for periodic testing and revision of contingency plans. Through the IT consultant, the Security Officer can:

a. Conduct one or more of the following exercises to test *Heiden Chiropractic Inc.*'s Contingency Plans (to include backup, disaster recovery, and emergency mode operations plans):

i) Tabletop exercises of response to specific scenarios;

ii) Technical restoration activities (including alternate site activities);

iii) Supplier facility and or service tests; or,

iv) Complete drills of the plan components.

b. Revise the Contingency Plan to address any deficiencies discovered during the testing activities and/or address necessary changes involving personnel, contact information, suppliers, legislation, or business risks, processes or strategies

c. Conduct testing and revision every year, or when there are significant changes to the environment.

7. Facility and IT Access

a. Physical and Technical Safeguards Policy[37]

The following physical safeguards shall be implemented:

1. *Heiden Chiropractic Inc.* will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. [38]

[36] 45 CFR § 164.308(7)(ii)(D). Addressable.
[37] *See* 45 C.F.R. § 164.310; 45 C.F.R. § 164.312. Required.
[38] S*ee* 45 C.F.R. § 164.310(a)(1). Required.

The Facility Security Plan serves as the master plan for safeguarding facilities and premises from unauthorized physical access. All repairs and modifications to the physical components of a facility shall be documented and maintained by *Heiden Chiropractic Inc.*'s Security Officer. All installation, repairs, and maintenance to computer hardware and software shall be documented and maintained by the IT consultant. The IT consultant shall conduct a review of all maintenance occurring on computer hardware and software on a monthly/quarterly/annual basis [CHOOSE ONE], and they shall conduct tests of the security attributes of all computer hardware and software as requested by the Security Officer. *Heiden Chiropractic Inc.*'s Security Officer shall maintain documentation of all repairs and modifications to computer hardware and software.

b. Procedures for validating workforce access to facilities:[39]

1. Configure facility access controls to allow employees access based on need. Only those employees of *Heiden Chiropractic Inc.* who need access to the office shall have a key to that office.

a. These employees should include those staff that retain an office in the building.

b. To the extent that employees have a key to access the building, such key should not be able to open any interior offices within the main building.

c. All offices containing protected health information shall be locked when not in use.

d. Patient files, both current and archived, shall be locked at all times when not in use.

2. Include a means to update the facility access control settings to reflect employee status changes.

c. Establish Security Maintenance Records[40]

1. Identify the physical components of the facility that are relevant to security (e.g., hardware, walls, doors and locks).

2. *Heiden Chiropractic Inc.*'s Security Officer must first approve any security-relevant physical modifications. *Heiden Chiropractic Inc.*'s Security Officer must oversee any modifications.

[39] *See* 45 C.F.R. § 164.310(a)(2)(iii). Addressable.
[40] *See* 45 C.F.R. § 164.310(a)(2)(iv). Addressable.

3. Create a maintenance record or log format; ensure it is updated for each modification and securely stored. Document all changes made to the physical location of the machines and installation of locks on cabinets and doors.

4. Ensure proper chain-of-custody for pertinent items (e.g., keys, access codes).

5. The policies and procedures established herein, including all derivative documents regarding the Facility Security Plan will be documented and maintained in a current manner by the Security Officer.

6. Store all HIPAA compliance documentation in a HIPAA compliance file.

d. Establish Device and Media Controls.[41]

1. *Heiden Chiropractic Inc.*'s Security Officer will inventory all hardware and electronic media containing EPHI, including all devices and electronic media that contain EPHI whether owned by *Heiden Chiropractic Inc.* or others. All devices and electronic media will be secured in a locked environment whenever possible, and a sign-out procedure will be implemented for all devices and electronic media. All returns will be strictly monitored and sign-out violations may result in sanctions.

2. Devices and electronic media containing EPHI must have access controls to prevent unauthorized access.

3. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for providing security awareness and training to all users of devices or electronic media containing EPHI regarding HIPAA's Security Rule requirements.

4. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for creating, maintaining and retaining documentation relating to the regulation and use of devices and electronic media containing EPHI. The documentation will be retained for at least six (6) years from the date of creation.

5. Disposal Procedures[42]

a. Under no circumstances will records associated with any open investigation, audit or litigation be destroyed.

[41] *See* 45 C.F.R. § 164.310(d)(1). Required.
[42] *See* 45 C.F.R. § 164.310(d)(2)(i). Required.

b. Disposal of records containing protected health information must prevent unauthorized access to protected health information through the use of shredding, erasing, modification, or another equally effective means.

c. When it is determined that information destruction is necessary, the subject data will be permanently destroyed; mere file deletion is not sufficient.

d. When an external company is hired to destroy EPHI the following is required:

i) Prior to transfer of information for destruction, shred, erase or modify protected health information to the extent possible.

ii) Have a Business Associate Agreement that meets the requirements set forth in the Privacy and Security Rules.

iii) Have the Business Associate submit proof of destruction and an assurance that all state and federal rules were met throughout the course of that destruction process.

e. *Heiden Chiropractic Inc.*'s Security Officer will document all disposal activities and maintain all documentation relating to disposal and retain the documentation for at least six (6) years from the date of creation. Documentation will include a permanent index of all destroyed records, including date and method of destruction, patient name, date of birth, last date of service (or inclusive dates of service); and, an attestation of destruction (may be signature of individual witnessing destruction).

6. Media Re-Use Procedures[43]

a. *Heiden Chiropractic Inc.* shall, through its Security Officer and to the extent applicable, implement procedures for removal of EPHI from electronic media before the media are made available for re-use.

b. All EPHI that must be retained will be transferred to other media and, before any EPHI is removed, the employee will confirm and document that such EPHI has been copied or moved.

c. Deletion or reformatting processes are permissible for preparing media for re-use, however, deleting and reformatting may not

[43] *See* 45 C.F.R. § 164.310(d)(2)(ii). Required.

always be sufficient to protect against access by an unauthorized user with specialized software. All optical media, such as a CD, must be destroyed, as these items cannot be reused.

d. *Heiden Chiropractic Inc.*'s Security Officer will document all activities related to preparing electronic media for re-use and maintain and retain such documentation for at least six (6) years from the date of its creation.

7. Data Backup and Storage Procedures[44]\

a. *Heiden Chiropractic Inc.* shall, through its Security Officer, create and implement retrievable exact copies of EPHI when needed, before movement of equipment. Backup data will be implemented and will occur near the time of movement, when possible.

b. Backup data will be stored in a secure environment, offsite from *Heiden Chiropractic Inc.*'s building.

c. Documentation of the data backup process will be performed at the same time as the data backup, and documentation is also required if data backup does not occur. The individual performing the backup will be responsible for this documentation and will include the date, identification of equipment to be moved, identification of data contained on the equipment and the individual instituting data backup or a reason why data backup did not occur. (See *Data Backup and Storage Form*). Such documentation will be copied and maintained by the Security Officer for at least six (6) years from the date of creation.

8. Protection from Malicious Software Procedures[45]

a. *Heiden Chiropractic Inc.*, through its Security Officer, shall develop, implement and monitor protection from malicious software including procedures for guarding against, detecting and reporting malicious software.

b. Guidelines for Virus Protection

i) *Heiden Chiropractic Inc.*'s computers will have anti-virus software installed and scheduled to run at regular intervals, updated as often as necessary to maintain protection.

[44] *See* 45 C.F.R. § 164.310(d)(2)(iv). Addressable.
[45] *See* 45 C.F.R. § 164.308(a)(5)(ii)(B). Addressable.

ii) Virus-infected computers will be removed from the network until verified as virus-free.

iii) Activities that intentionally create and/or distribute malicious programs into the network are prohibited and such activity by an employee will result in immediate disciplinary action.

iv) *Heiden Chiropractic Inc.*'s workforce shall be prohibited from opening files or macros attached to any e-mail that look unusual or are from an unknown source and may not forward spam, chain or other junk e-mail. These emails should be deleted and the trash emptied.

v) *Heiden Chiropractic Inc.* may also implement requirements necessitating the scanning of external data sources, such as floppy disks, thumb drives and CDs, before use and the regular backup and storage of data.

9. Evaluation Procedures[46]

a. *Heiden Chiropractic Inc.* shall, through its Security Officer, develop and implement a process facilitating the performance of periodic technical and non-technical evaluations, based initially upon the standards of the HIPAA Security Rule Requirements and subsequently, in response to environmental or operational changes affecting the security of EPHI.

b. The security policies and procedures will be reviewed annually and may be structured for review on a monthly basis.

c. A technical evaluation should be performed by *Heiden Chiropractic Inc.*'s IT consultant and done on a scheduled basis thereafter. These evaluations include full on-site and remote evaluations of all systems and the network. From these evaluations the IT consultant creates a technology summary, SWOT analysis and IT budget. The evaluation should include assessments to ensure that policies and procedures have been developed and implemented in compliance with the HIPAA Security Rule Requirements and are functioning in a manner to protect confidentiality, integrity and availability of EPHI. The effectiveness of security policies and procedures are also reviewed periodically.

[46] 45 CFR § 164.308(a)(8). Required.

d. Subsequent evaluations may be based on analyses of security incidents, changes in practice and new technology.

e. Evaluations may need to be performed periodically as a result changes in the Security or Privacy Rules; new federal, state or local regulations affecting the privacy and/or security of protected health information; changes in environmental and/or business processes or operations that may affect security safeguards; and/or a serious security threat or incident.

f. *Heiden Chiropractic Inc.*'s Security Officer will implement any necessary changes and shall be responsible for documentation, maintenance and retention of any information relating to periodic evaluations of security policies and procedures including periodic evaluation reports, analyses, recommendations and/or changes made. Such documentation will be maintained for at least six (6) years from the date of creation.

10. Access control[47]

Heiden Chiropractic Inc., through its Security Officer or delegated system administrator, implement and monitor technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in *Heiden Chiropractic Inc.*'s *Authorization of Access to EPHI Procedure.*

Access controls will be established through system administrator accounts and intended to regulate the authorized user access according to the person or class of persons and functions they perform and will include the use of unique user identifications (whether names or numbers), emergency access procedures, automatic log-off mechanisms, and encryption and decryption mechanisms. Access control may be accomplished through the use of a variety of software tools and, at the discretion of its Security Officer, *Heiden Chiropractic Inc.* may work with a vendor or health information technician to determine what controls are available to the provider based on their information system. *Heiden Chiropractic Inc.* will seek to implement only health information technology and methodologies that meet the standards adopted by DHHS pursuant to Section 13101 of the HITECH Act.

a. Technical access controls will be implemented based on authorization of access determined in Access Authorization Policy and Procedures.

[47] *See* 45 C.F.R. § 164.312(a)(1). Required.

b. The privileges provided to system administrator accounts will permit the system administrator to add new user accounts, modify existing user accounts or terminate accounts. The system administrator account provides full access to the operating system, applications, system files privacy protected data files and audit trails.

c. *Heiden Chiropractic Inc.*'s IT Consultant will be responsible for documenting all activities related to technical access controls, including all system administration activities. *Heiden Chiropractic Inc.*'s Security Officer will ensure that such documentation is maintained and retained for at least six (6) years from the date of creation.

e. Unique User Identification[48]

Heiden Chiropractic Inc. shall, through its Security Officer, implement policies and procedures to assign a unique name and/or number for identifying and tracking user identity.

1. Unique user identifications are created in accordance with the Authorization of Access to EPHI Procedure.

2. When requesting access to any network, system or application that accesses, transmits, receives or stores EPHI, a user or employee will be required to supply their assigned unique user identification in conjunction with a secure password to gain access to the above-mentioned networks, systems or applications.

3. The employees or other authorized persons who are assigned unique access codes will be required to follow practices that maintain unique tracking capabilities and uniqueness of the code.

4. It is the responsibility of the user or employee to maintain their unique user identification in a protected manner and to ensure that it is only used for authorized access to networks, systems or applications. Compromise to the security of the unique user identification by a user or employee must be immediately reported to the Security Officer.

5. A lost password or unique user ID must be reported immediately to the Security Officer and authorized access must be terminated.

6. Failure to comply with these policy and procedures may result in immediate disciplinary action.

[48] *See* 45 C.F.R. § 164.312(a)(2)(i). Required.

7. *Heiden Chiropractic Inc.*'s Security Officer is responsible for reviewing and evaluating this policy and procedure on a periodic basis to ensure that they maintain technical compliance.

8. *Heiden Chiropractic Inc.*'s Security Officer will be responsible for documenting all activities that relate to assignment and use of unique user identification. The documentation will be maintained and retained for a minimum of six (6) years from the date of creation.

f. Automatic Log-Off[49]

1. The automatic log-off procedure is addressed in the Employee Use of EPHI Procedures.

g. Encryption and Decryption[50]

1. To the extent possible, *Heiden Chiropractic Inc.* shall, through its Security Officer, implement a mechanism to encrypt and decrypt EPHI.

2. *Heiden Chiropractic Inc.*'s Security Officer will determine the extent to which encryption and decryption mechanisms will be implemented by *Heiden Chiropractic Inc.* and document his/her analysis and conclusions regarding the same.

3. *Heiden Chiropractic Inc.*'s Security Officer will document all activities related to encryption and decryption. The documentation will be maintained for at least six (6) years from the date of creation.

8. Vendor and Contractor Access[51]

It is *Heiden Chiropractic Inc.* policy that all vendors ("Business Associates") and contractors[52] sign an agreement regarding the security of EPHI under which *Heiden Chiropractic Inc.* may permit a person meeting the definition of a "Business Associate"

[49] *See* 45 C.F.R. § 164.312(a)(2)(iv). Addressable.
[50] *See* 45 C.F.R. § 164.312(a)(2)(iv). Addressable.
[51] 45 C.F.R. § 164.308(b)(1).
[52] "Contractor" of the *[NAME OF COVERED ENTITY]* has the same meaning as "Business Associate" of a Covered Entity under HIPAA, 45 CFR § 160.103, which defines "Business Associate" as an entity that works on behalf of *[NAME OF COVERED ENTITY]*, other than in the capacity of a member of the workforce of *[NAME OF COVERED ENTITY]*, performs, or assists in the performance of: (A) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) any other function or activity regulated by HIPAA; or provides, other than in the capacity of a member of the workforce of *[NAME OF COVERED ENTITY]*, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for *[NAME OF COVERED ENTITY]*, where the provision of the service involves the disclosure of individually identifiable health information from *[NAME OF COVERED ENTITY]* or from another Business Associate of *[NAME OF COVERED ENTITY]* to the entity.

under HIPAA to create, receive, maintain and/or transmit EPHI upon *Heiden Chiropractic Inc.*'s receipt of satisfactory assurances from the Business Associate that it will appropriately protect and safeguard the information.

a. The Business Associate Agreement will comply with HIPAA privacy and security rules and state that the Business Associate will:

    1. Abide by *Heiden Chiropractic Inc.*'s privacy and security practices.

    2. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that it creates, receives, maintains or transmits on behalf of *Heiden Chiropractic Inc.*.

    3. Be responsible for ensuring that any persons and agents (including subcontractors) to whom the Business Associate provides PHI will agree to the same restrictions.

    4. Report to *Heiden Chiropractic Inc.* any violations of the agreement's terms, prohibitions and restrictions, in accordance with the notice of breach requirements in the HITECH Act and *Heiden Chiropractic Inc.*'s Notice of Breach policy and procedure.

    5. Be terminated if *Heiden Chiropractic Inc.* determines that the Business Associate has violated a material term of the Agreement.

b. Written Contract With Other Contractors[53]

    1. *Heiden Chiropractic Inc.*'s Security Officer will obtain satisfactory assurances from *Heiden Chiropractic Inc.*'s Contractors that the Contractors will appropriately safeguard protected health information.

    2. *Heiden Chiropractic Inc.*'s Security Officer will obtain such satisfactory assurances through a Business Associate Agreement that meets the requirements in the HIPAA Security Rule, outlined in 45 CFR § 164.314(a) and the new HITECH requirements. See *Model Business Associate Agreement Form*.

[53] 45 C.F.R. § 164.308(b)(1). Required.

HIPAA PRIVACY POLICIES AND PROCEDURES

Introduction – HIPAA Privacy Policy

As a HIPAA covered entity, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 CFR Parts 160 and 164) ("HIPAA") restrict *Heiden Chiropractic Inc.*'s ability to use and disclose protected health information ("PHI"). PHI means information that is created or received by *Heiden Chiropractic Inc.* and relates to the past, present, or future physical or mental health or condition of a client; the provision of health care to a client; or the past, present, or future payment for the provision of health care to a client; and that identifies the client or for which there is a reasonable basis to believe the information can be used to identify the client. PHI includes information of persons living or deceased.

It is *Heiden Chiropractic Inc.*'s policy to comply fully with HIPAA's requirements and any amendments thereto. *Heiden Chiropractic Inc.* recognizes that all members of its workforce may have access to PHI. Accordingly, all members of *Heiden Chiropractic Inc.*'s workforce must comply with this Privacy Policy and all related procedures. The term "workforce," as defined under HIPAA, includes those employees, volunteers, trainees, and other persons whose work performance is under the direct control of *Heiden Chiropractic Inc.*, whether or not they are paid by *Heiden Chiropractic Inc.*, and whose job entails the use, maintenance or disclosure of PHI.

No third party rights are intended to be created by this Policy. *Heiden Chiropractic Inc.* reserves the right to amend or change this Policy at any time (even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational but not be binding upon *Heiden Chiropractic Inc.*. This Policy does address requirements under other federal laws or under state laws.

POLICIES AND PROCEDURES REGARDING *Heiden Chiropractic Inc.*'S RESPONSIBILITIES AS COVERED ENTITY

1. Privacy Official Designation

[CONTACT FOR NAME OF COVERED ENTITY] will be the Privacy Official for *Heiden Chiropractic Inc.*. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and any implementing Procedures. The Privacy Official will also act as the contact person for clients who have questions, concerns, or complaints about the privacy of their PHI.

2. Training

It is *Heiden Chiropractic Inc.*'s policy to train all members of its workforce on its privacy policies and procedures. The Privacy Official (directly or through the Privacy Official's staff) is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within *Heiden Chiropractic Inc.*. Training procedures include:

a. Conduct initial training of all workforce members upon implementation of these policies and procedures.

   1. Initial training must include review of all new forms that will be used by *Heiden Chiropractic Inc.*, who is responsible for using them, why they are used and when they are used.

   2. *Heiden Chiropractic Inc.* may decide to hire an outside organization to conduct the initial training about the HIPAA privacy rules.

   3. Staff will sign an acknowledgement form indicating that they received training in the HIPAA privacy rules and *Heiden Chiropractic Inc.*'s policies and procedures regarding those rules.

   4. The signed Acknowledgement form shall be kept in each employee's personnel file for a period of at least six years.

b. Conduct follow-up training to selected employees who are affected by changes to these policies and procedures as a result of an internal practice change or change in the law.

   1. *Heiden Chiropractic Inc.* may hire an outside organization to conduct follow-up training about the changes to the HIPAA privacy rules.

   2. Staff who is selected for follow-up training must sign an Acknowledgement form, which will be kept in the employee's personnel file for a period of at least six years.

3. Technical, Physical and Administrative Safeguards

In accordance with the Security Safeguards, *Heiden Chiropractic Inc.* will establish the appropriate technical and physical safeguards to prevent PHI from being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and positioning paper and electronic PHI to limit incidental disclosures.

Administrative safeguards include firewalls, which will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for *Heiden Chiropractic Inc.*'s administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

a. The procedure for technical, physical and administrative safeguards is:

    1. Conduct an initial assessment of the technical, physical and administrative safeguards needed by *Heiden Chiropractic Inc.* to ensure the most protection of PHI.

        a. Appoint or hire staff to review current protections provided to PHI. Tour facilities, test technical safeguards, review policies authorizing PHI access.

        b. Create a gap analysis to identify areas that need improvement.

        c. Implement changes in accordance with the gap analysis.

    2. Periodically review and test the safeguards to ensure continued compliance.

    3. Update safeguards in response to technical, staff or facility changes.

    4. Maintain gap analysis and documentation relating to safeguards in accordance with Documentation and Retention procedure.

b. Implementation of Standards and Methodologies Set by the Secretary[54]

    1. In order to further the goal of electronic exchange of health information and to maintain the privacy and security of that information, *Heiden Chiropractic Inc.* intends to adopt the information technology standards and methodologies suggested or required by the Secretary through guidance, regulations or rules.

[54] HITECH §§ 13401-13402.

2. *Heiden Chiropractic Inc.*, through its Privacy and/or Security Officer, will monitor the Department of Health and Human Services website and/or regularly consult HIPAA experts for new guidance or rules that are issued by the Secretary related to standards or methodologies that protect the privacy or security of PHI.

3. *Heiden Chiropractic Inc.* agrees to adopt the recommended or required technologies, methodologies and standards provided in any guidance, regulations or rules issued by the Secretary.

4. Privacy Policy Notice, Complaints, and Sanctions

a. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of *Heiden Chiropractic Inc.*'s privacy practices that describes the uses and disclosures of PHI that may be made by *Heiden Chiropractic Inc.*, the individual's rights, and *Heiden Chiropractic Inc.*'s legal duties with respect to the PHI. *Heiden Chiropractic Inc.* cannot use or disclose any PHI except in accordance with the current Notice of Privacy Practices (the "Notice"). The Notice will also inform individual's about their rights of access to their PHI, their right to request amendments be made if the individual feels the PHI is inaccurate, and their right to obtain an accounting of disclosures that have occurred without an authorization.

The Notice will inform clients that *Heiden Chiropractic Inc.* will have access to PHI in connection with its treatment, payment and administrative functions. The Notice will also provide a description of *Heiden Chiropractic Inc.*'s complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The Notice will be individually delivered to all *Heiden Chiropractic Inc.* clients at the time of the client's initial visit with *Heiden Chiropractic Inc.* and within sixty (60) days after a material change to the notice. The procedure for Notice of privacy practices is:

1. Consult 45 CFR § 164.520 and draft the Notice of Privacy Practices accordingly, ensuring each requirement is included in the Notice. See Notice of Privacy Practices form.

    a. *Heiden Chiropractic Inc.* may use Notices drafted by other organizations, and then tailor the templates to fit the needs of *Heiden Chiropractic Inc.*. In such cases, *Heiden Chiropractic Inc.* will ensure that the appropriate state and federal laws are addressed and may seek legal counsel to review for compliance.

2. Consult any state laws that might apply to the Notice and incorporate accordingly.

3. Make the Notice available through *Heiden Chiropractic Inc.*'s website.

4. Provide the initial Notice to all clients.

5. Make a good faith effort to have clients sign a written acknowledgment of receiving the Notice. See Acknowledgement of Receipt of Privacy Notice form. If *Heiden Chiropractic Inc.* is unable to get a signed written acknowledgment form, document in the patient's record why the acknowledgment was not obtained.

6. Provide the Notice to all new clients as part of the enrollment packet.

7. Revise the Notice in response to any relevant internal practice or law changes. Within 60 days of a material revision, provide the revised Notice once those changes are in effect.

8. Every three years from the date of the initial Notice roll out, *Heiden Chiropractic Inc.* will notify clients of the availability of the Notice and how to obtain a copy of the Notice.

9. Maintain each version of the Notice for six years and in accordance with the Document and Retention Policy and Procedure.

b. Complaints

Heiden Chiropractic Inc. shall provide a process for the client to file a complaint if the client feels his or her privacy rights have been violated. The client may also file a complaint concerning *Heiden Chiropractic Inc.*'s privacy policies and procedures, even without alleging a violation of rights. A copy of the complaint procedure shall be provided to any client upon request.

[CONTACT FOR NAME OF COVERED ENTITY] will be *Heiden Chiropractic Inc.*'s contact person for receiving complaints, and shall establish a process for receiving, investigating and responding to client complaints. The client complaint process shall be described in *Heiden Chiropractic Inc.*'s Notice of Privacy Practices. *Heiden Chiropractic Inc.* also recognizes the client's right to file a complaint with the federal Department of Health and Human Services. *Heiden Chiropractic Inc.* shall cooperate with a federal investigation of the client's complaint.

Any intimidation of or retaliation against clients, families, friends, or other clients in the complaint process is prohibited. Employees who violate this policy are subject to disciplinary action, up to and including termination.

If the client's rights have been violated, employees who violated those rights are subject to disciplinary action, up to and including termination. *Heiden Chiropractic Inc.* shall mitigate, to the extent feasible, any known harmful effects of the violation. The procedure for complaints is:

1. Filing a Complaint

    a. A client may call, write, or present in person to the Privacy Officer or designated person the alleged privacy violation or complaint by either *Heiden Chiropractic Inc.* or one of *Heiden Chiropractic Inc.*'s Business Associates.

    b. The Privacy Officer or designated person will summarize the complaint on the Client Complaint Report Form.

2. Investigation of Complaint

    a. The Privacy Official or designated person will facilitate the investigation of the complaint.

3. Response to Complaint

    a. A written response will be provided to the client within 30 days from the date the complaint was filed.

    b. A written summary of the complaint and action taken will be filed with the Privacy Official.

4. Translators, interpreters, and readers who meet the communication needs of the client may be provided during the complaint process.

5. Clients are permitted to have a representative of their choice to represent their interests during the complaint process.

6. Occurrences representing potential liability claims will be referred to Risk Management.

7. Clients who request an outside agency to review their complaint may contact the Secretary of the federal Department of Health and Human Services at 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.

8. Documentation

    a. All complaints received must be documented.

    b. All complaint dispositions must be documented.

    c. The documentation must be retained for six years.

c. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with *Heiden Chiropractic Inc.*'s discipline policy, which includes termination. The sanctions procedure is:

1. Anyone subject to *Heiden Chiropractic Inc.*'s discipline policy as written in *Heiden Chiropractic Inc.*'s employee handbook shall be subject to said discipline for violating any of these policies and procedures.

2. Anyone who becomes aware of a *Heiden Chiropractic Inc.* employee or agent violating these policies and procedures shall report the violation to the Privacy Officer, either in writing or verbally.

3. The Privacy Officer will conduct an investigation of the violation, interviewing the subject of the complaint as well as other employees or agents for information gathering purposes.

4. The Privacy Officer shall write a report regarding the complaint and share it with the subject individual's supervisor.

5. In consultation with the Privacy Officer, the supervisor shall determine the appropriate level of discipline in accordance with the disciplinary procedures found in the employee handbook.

6. Intentional violations of these policies and procedures shall be addressed with more strict discipline, up to and including termination.

7. Inadvertent violations shall be assessed in accordance with *Heiden Chiropractic Inc.*'s disciplinary procedures.

8. The Privacy Officer shall assess with each alleged violation whether the violation is widespread across *Heiden Chiropractic Inc.* or whether it is an isolated event. In the case of the former, the Privacy Officer shall educate *Heiden Chiropractic Inc.*'s workforce on how to avoid such violations in the future and modify these policies and procedures, as well as other *Heiden Chiropractic Inc.* practices, accordingly.

9. All complaints and associated documentation shall be maintained for six years, in accordance with the Document and Retention Policy and Procedure.

d. No Intimidating or Retaliatory Acts

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility. The procedure for preventing intimidation or retaliatory acts is:

1. Whenever a *Heiden Chiropractic Inc.* employee voices a complaint regarding the HIPAA privacy rules or these policies and procedures, either through oral or written form, internally or externally, *Heiden Chiropractic Inc.* shall address the concern voiced by the employee in a positive and constructive manner by asking the Privacy Officer to investigate the complaint to determine its legitimacy.

2. If the complaint is legitimate, the Privacy Officer shall follow *Heiden Chiropractic Inc.*'s complaint policy and procedure.

3. Regardless of the concern expressed by the employee, *Heiden Chiropractic Inc.* shall not base any action or decision regarding the employee's employment, safety or well-being on the employee's decision to voice the concern. *Heiden Chiropractic Inc.* will encourage an open dialogue regarding HIPAA privacy compliance.

e. No Waiver of HIPAA Privacy

1. *Heiden Chiropractic Inc.* shall not make any treatment, payment, health care operations or eligibility decisions based upon a patient's ability or desire, expressed or not, to invoke their rights under HIPAA.

    a. These rights include an individual's desire or ability to file a complaint to the Secretary of the Department of Health and Human Services about any perceived HIPAA violation.

f. Documentation and Retention

Heiden Chiropractic Inc.'s security and privacy policies and procedures shall be documented and all policies and procedures shall be retained for at least six (6) years from the date of issue. All security actions that must be documented will be recorded in either paper or electronic form. Documentation will be available to all employees and the location of such documentation will be conveyed during training on the HIPAA security and privacy rules.

Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, implementation specifications (including changes and modifications in regulations), and environmental or operational changes. *Heiden Chiropractic Inc.* will review periodically all

security and privacy documentation and update as necessary. Any changes to policies or procedures must promptly be documented. If a change in law affects the Notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the Notice. *Heiden Chiropractic Inc.* shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities such as *Heiden Chiropractic Inc.* must maintain such documentation until the later of six (6) years from the date of its creation or the date when it was last in effect. The procedure for documentation and retention of records is:

1. The Privacy Officer shall be responsible for maintaining all documents, either in paper or electronic form.

2. The Privacy Officer shall designate a place within *Heiden Chiropractic Inc.* to store paper documents relating to HIPAA privacy and a place within *Heiden Chiropractic Inc.*'s computer system to store electronic documents. The Privacy Officer shall inform all employees of where these policies and procedures are housed so the employees may reference them when necessary.

3. All documentation shall be kept for six years. The Privacy Officer shall create an inventory system to track the retention period for all HIPAA-related documents.

4. After six years of retention, a document may be destroyed in accordance with *Heiden Chiropractic Inc.*'s document destruction policy and procedure.

5. Whenever a change in *Heiden Chiropractic Inc.*'s policies and procedures affect the provisions of the Notice of Privacy Practices, *Heiden Chiropractic Inc.* shall update the Notice to reflect the change and follow the Notice policy and procedure in notifying and distributing the updated Notice.

6. The Privacy Officer will monitor bi-annually the HIPAA security and privacy documentation to ensure it is up to date.

7. Whenever there is a change in law, standards, requirements, implementation specifications (including changes and modifications in regulations), environment or operation, the Privacy Officer will update the security and privacy policies and procedures accordingly.

5. Breaches

a. Inadvertent Disclosures of PHI

Heiden Chiropractic Inc. shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a disclosure of PHI, either by an employee of *Heiden Chiropractic Inc.* or an outside consultant/contractor that is not in compliance with this Policy, the employee shall immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the client can be taken. The procedure to mitigate any inadvertent disclosures of PHI is:

1. When a violation of these policies and procedures is discovered, whether through an internal or external complaint or audit, the Privacy Officer shall be notified.

2. The Privacy Officer shall investigate the violation by determining how it occurred, the frequency of the violation, who was impacted by the violation and when the violation occurred. The Privacy Officer shall document his or her findings.

3. Based upon those findings, the Privacy Officer shall take the appropriate steps to ensure that such violations do not occur in the future and to ensure that the violation does not continue to spread.

4. In the case of a breach of privacy of PHI, *Heiden Chiropractic Inc.* shall follow the procedures set forth in the Notice of Breach Policy and Procedure.

5. In the case of an employee violation, the Privacy Officer shall consult the Sanctions Policy and Procedure and respond accordingly.

6. The Privacy Officer shall document all mitigation efforts and retain for six years and in accordance with the Document and Retention Policy and Procedure.

b. Notice of Breach Policy [55]

Heiden Chiropractic Inc. shall, through its Privacy Officer, ensure that the appropriate entities and persons are aware of security breaches that may undermine the privacy of the Individuals' PHI so that mitigation of the incident can occur as soon as possible after the incident.

[55] 45 C.F.R., Subpart D.

1. A "breach" is the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.

2. A "breach" does not include:

    a. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of *Heiden Chiropractic Inc.* if-

        i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the Individual; and

        ii) the information is not further acquired, access, used, or disclosed in a manner not permitted by the HIPAA Privacy Rule.

    b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by *Heiden Chiropractic Inc.* to another similarly situated individual at the same facility and any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.

    c. A disclosure where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure is made would not reasonably have been able to retain such information.

3. *Heiden Chiropractic Inc.* will work to ensure that it uses Secured PHI, such as encrypting all EPHI still in use and destroying the media on which the PHI is stored or recorded when the PHI no longer needs to be retained.[56] *Heiden Chiropractic Inc.* acknowledges that a breach of "secured" PHI is not subject to any notice requirements under HITECH.

---

[56] "Unsecured protected health information" means PHI that has been encrypted or destroyed. *See* 74 Fed. Reg. 42742 (August 24, 2009). EPHI has been encrypted by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. *Id.* Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, available at http://www.csrc.nist.gov/. *Id.* Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. *Id.* These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated. *Id.* Available at http://www.csrc.nist.gov/. As for PHI destruction, paper, film, or other hard copy media should be shredded or destroyed so that the PHI cannot be read or otherwise reconstructed. *Id.* For electronic media, destruction includes clearing, purging or destroying consistent with NIST Special Publication 800-88, Guidelines for Media

(footnote continued)

4. *Heiden Chiropractic Inc.*, through its Privacy Officer, will regularly monitor guidance or rules issued by DHHS to determine what the Secretary considers Secured PHI, or PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals.[57]

c. Procedure for Breach of Unsecured PHI

1. To determine if an impermissible use or disclosure of PHI constitutes a breach, *Heiden Chiropractic Inc.* will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure.[58] The risk assessment shall be fact specific and shall address:

a. the nature's extent of PHI involved, including the types of identifiers and likelihood of reidentification;

b. the unauthorized person who used the PHI or to whom the disclosure was made;

c. whether the PHI was actually acquired or viewed; and

d. the extent to which the risk to PHI has been mitigated.

2. If it is determined that a breach has occurred and that it involves the access, acquisition or disclosure of "unsecured protected health information" by either *Heiden Chiropractic Inc.* or one of *Heiden Chiropractic Inc.*'s Business Associates, unless Paragraph 7 (below) applies, *Heiden Chiropractic Inc.* will notify each Individual whose unsecured PHI has been, or is reasonably believed by *Heiden Chiropractic Inc.* to have been, accessed, acquired, or disclosed as a result of such breach. *Notice of Breach Letter to Individuals*.

a. The notice from a Business Associate to *Heiden Chiropractic Inc.* will include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired or disclosed during such incident.

b. Notice from *Heiden Chiropractic Inc.* to Individuals affected by the breach shall be delivered using the following methods:

Sanitization, such that the PHI cannot be retrieved. *Id.* This guidance may change. It is [Entity's] intent to implement whatever guidance DHHS issues so it may fall within the safe harbor of "secured PHI." The HITECH Act § 13402(h).

[57] The HITECH Act § 13402(h)(2).

[58] 74 Fed. Reg. 42744 (Aug. 24, 2009).

i) Written notification by first-class mail to the Individual (or the next of kin of the Individual if the Individual is deceased) at the last known address of the Individual or the next of kin, respectively, or, if specified as a preference by the Individual, by electronic mail. The notification may be provided in one or more mailings as information is available. *Notice of Breach Letter to Individuals.*

ii) If there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that prevents direct written (or electronic, if specified by the Individual) notification to the Individual, *Heiden Chiropractic Inc.* shall provide a substitute form of notice. Such notice in media or web posting will include a toll-free phone number active for at least 90 days where an Individual can learn whether the Individual's unsecured PHI is possibly included in the breach. If there are 10 or more Individuals for which there is insufficient or out-of-date contact information, this substitute notice shall include either:

(A) A conspicuous posting for a period of 90 days on the home page of *Heiden Chiropractic Inc.*'s web site; or

(B) Conspicuous notice in a major print or broadcast media, including major media in a geographic area where the Individuals affected by the breach likely reside; and

iii) If *Heiden Chiropractic Inc.* determines that urgency in notification of Individuals exists because of a possible imminent misuse of unsecured PHI, *Heiden Chiropractic Inc.*, in addition to the notice provided by one of the methods in Paragraphs 1 or 2 above, may provide information to Individuals by telephone or other means, as appropriate.

c. Regardless of the method used to provide notice to Individuals, the content of the notice shall be in plain language and include the following:

i) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii) A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, or disability code);

iii) The steps Individuals should take to protect themselves from potential harm resulting from the breach. *See Notice of Breach Letter to Individuals* for examples;

iv) A brief description of what *Heiden Chiropractic Inc.* is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and

v) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free number, an email address, web site, or postal address.

3. Unless Paragraph 7, below, applies, if the breach involves the unsecured PHI of more than 500 residents of a certain region or jurisdiction, or is reasonably believed to have been accessed, acquired or disclosed during such breach, *Heiden Chiropractic Inc.* will notify the prominent media outlets that serve the geographic area or jurisdiction affected. *See Notice of Breach Press Release*.

4. Unless Paragraph 7, below, applies, if the breach involves the unsecured PHI of more than 500 Individuals, *Heiden Chiropractic Inc.* will immediately notify the Secretary by filling out the form provided on the DHHS website at www.hhs.gov/ocr/privacy//hipaa/administrative/breachnotificationrule/brinstruction.html. *Heiden Chiropractic Inc.* understands that the Secretary will make available to the public on the DHHS web site a list that identifies each covered entity involved in a breach in which the unsecured PHI of more than 500 Individuals is acquired or disclosed.

5. Unless otherwise specified, *Heiden Chiropractic Inc.* and its Business Associates will provide all notices required by this policy without reasonable delay or the notification within 60 calendar days after discovery of the incident, whichever is shorter.

6. *Heiden Chiropractic Inc.* will document each breach using the *Notice of Breach Form* and use this form when submitting its annual report to the Secretary not later than 60 days after the end of each calendar year in which there is a breach involving fewer than 500 individuals. The form is available at www.hhs.gov/ocr/privacy//hipaa/administrative/breachnotificationrule/brinstruction.html.

7. *Heiden Chiropractic Inc.* will delay notifying Individuals, the media, and the Secretary, as outlined above, if a law enforcement official determines

that a notification, notice, or posting would impede a criminal investigation or cause damage to national security.

a. The law enforcement official must make the request to delay notification in writing. If such request is not made in writing and is made orally only, *Heiden Chiropractic Inc.* will document the statement by the law enforcement official, including the identity of the agency or official making the statement, temporarily suspend the notification, and limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

8. Regardless of the notice requirements described above, *Heiden Chiropractic Inc.* will mitigate the effects of the breach in security and privacy of PHI to ensure that the incident is not repeated.[59]

9. *Heiden Chiropractic Inc.* will retain all documents related to breaches in security, including documentation regarding a delay in notification, risk management activities, copies of all notification letters to Individuals, DHHS and media, if applicable, and mitigation efforts for a period of no less than 6 years.

6. Procedures for Use and Disclosure of PHI

Heiden Chiropractic Inc. will use and disclose PHI only as permitted under HIPAA and other relevant state and federal laws, such as a state's confidentiality laws or the federal laws governing the confidentiality of alcohol and other substance abuse records. Employees and other individuals who are within the definition of "workforce" as defined above in this policy shall have access to PHI only to the extent necessary for the workforce members to carry out their duties. Nevertheless, all workforce members shall be subject to these policies and procedures.

The terms "use" and "disclosure" are defined as follows:

Use. The, sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any appropriately designated person working for or within *Heiden Chiropractic Inc.*, or by a Business Associate (defined below) of *Heiden Chiropractic Inc.*.

Disclosure. For information that is protected health information ("PHI"), disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working for *Heiden Chiropractic Inc.*.

a. Permitted Uses and Disclosures: Treatment, Payment and Health Care Operations

[59] See 45 CFR § 164.530(f).

PHI may be disclosed for *Heiden Chiropractic Inc.*'s own treatment, payment or health care operations purposes without the client's consent, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

1. Objective: To facilitate the use or disclosure of PHI for treatment, payment and health care operations purposes under circumstances permitted by HIPAA.

2. Definitions:[60]

    a. ***Treatment.*** Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

    b. ***Payment.*** Payment includes activities undertaken to obtain contributions or to determine responsibility for provision of benefits or to obtain reimbursement for health care. Payment also includes:

        i) Eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

        ii) Risk adjusting based on client status and demographic characteristics; and

        iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

    c. ***Health Care Operations.*** Health care operations means any of the following activities to the extent that they are related to *Heiden Chiropractic Inc.*'s administration:

        i) Conducting quality assessment and improvement activities;

        ii) Reviewing health provider performance;

[60] *See* 45 CFR § 164.501

iii) Conducting or arranging for medical review, legal services and auditing functions;

iv) Business planning and development; and

v) Business management and general administrative activities.

d. PHI may be disclosed for purposes of *Heiden Chiropractic Inc.*'s own treatment, payment or health care operations without the client's consent. PHI may be disclosed to another covered entity without the client's consent for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the client and the PHI requested pertains to that relationship.

3. Procedure for Treatment, Payment and Health Care Operations Disclosures

a. ***Uses and Disclosures for Treatment, Payment Activities or Health Care Operations.*** *Heiden Chiropractic Inc.*'s workforce may use and disclose *Heiden Chiropractic Inc.*'s client's PHI to perform *Heiden Chiropractic Inc.*'s own treatment, payment activities or health care operations.

i) Disclosures must comply with the "Minimum Necessary" Standard. Under that procedure, if the disclosure is not recurring and for which a specific disclosure procedure has been created, the disclosure must be approved by the Privacy Official.

ii) Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

b. ***Disclosures of PHI to Other Health Care Providers.*** *Heiden Chiropractic Inc.* will release client health care records upon request without informed consent including a health care provider or any person acting under the supervision of a health care provider or licensed emergency medical service personnel, including medical staff members, employees or persons serving in training programs or participating in volunteer programs and affiliated with the health care provider, to the extent that performance of their duties requires access to the records, if any of the following is applicable:

i) The person/provider is rendering assistance to the client;

ii) The person/provider is being consulted regarding the health of the client;

iii) The life or health of the client appears to be in danger and the information contained in the client health care records may aid the person/provider in rendering assistance; or,

iv) The person/provider prepares or stores records, for the purposes of the preparation or storage of those records.

v) Disclosures should be documented in accordance with the procedure for "Documentation and Retention."

c. ***Disclosures for Another Entity's Payment Activities***. *Heiden Chiropractic Inc.*'s workforce may disclose a client's PHI to another covered entity to perform the other entity's payment activities. Disclosures may be made under the following procedures:

i) Disclosures must comply with the "Minimum Necessary" Standard. Under that procedure, if the disclosure is not recurring and for which a specific disclosure procedure has been created, the disclosure must be approved by the Privacy Official.

ii) Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

d. ***Disclosures for Certain Health Care Operations of the Receiving Entity***. *Heiden Chiropractic Inc.*'s workforce may disclose PHI for purposes of another covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual who is the subject of the PHI and the PHI requested pertains to that relationship. Such disclosures are subject to the following:

i) The disclosure must be approved by the Privacy Official.

ii) Disclosures must comply with the "Minimum-Necessary" Standard.

iii) Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

e. ***Questions.*** If there are any questions or if any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of *Heiden*

Chiropractic Inc. should contact the Privacy Official. See 45 CFR § 164.506.

b. Mandatory Disclosures of PHI: to Individual and DHHS

A client's PHI must be disclosed as required by HIPAA in two situations: the disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows); and the disclosure is made to a governmental Department of Health and Human Services ("DHHS") for purposes of enforcing of HIPAA. *See* 45 CFR § 164.502(a)(2).

Objective: To facilitate disclosures when required by HIPAA to individuals upon request and to a governmental Department of Health and Human Services ("DHHS") for purposes of enforcing HIPAA.

1. Procedure for Mandatory Disclosures

a. ***Request from Individual.*** Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Allowing PHI Access to Individuals."

b. ***Request from DHHS.*** Upon receiving a request from a DHHS officer for disclosure of PHI, the employee must follow the procedures for verifying the identity of a public officer set forth in "Verification of Identity of Those Requesting Protected Health Information" and disclosures be documented in accordance with the procedure for "Documentation Requirements." *See* 45 CFR § 164.502(a)(2).

c. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

Depending upon state privacy laws, PHI may be disclosed in the following situations without a client's authorization when specific requirements are satisfied. *Heiden Chiropractic Inc.*'s disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the *Heiden Chiropractic Inc.*'s Privacy Official. Permitted are disclosures:[61]

- About victims of abuse, neglect or domestic violence;
- For judicial and administrative proceedings;

[61] *See* 45 CFR § 164.512.

- For law enforcement purposes;
- For public health activities;
- For health oversight activities;
- About decedents;
- For cadaveric organ, eye or tissue donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

Objective: To facilitate disclosures for legal and public policy purposes under circumstances permitted by HIPAA.

1. Procedure for Disclosures for Legal or Public Policy Purpose

    a. ***Disclosures for Legal or Public Policy Purposes***. An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made without the individual's written authorization if the following procedures are followed:[62]

        i) The disclosure must be approved by the Privacy Official.

        ii) Disclosures must comply with the "Minimum Necessary" Standard.

        iii) Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

        iv) The disclosure is not contrary to any other state or federal law regarding confidentiality

[62] See 45 CFR § 164.512.

2. Legal and Public Policy Disclosures

a. Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

i) The individual agrees with the disclosure; or

ii) The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

iii) In deciding whether the disclosure is expressly authorized by statute, *Heiden Chiropractic Inc.* will consult state confidentiality laws as well as federal AODA regulations under 42 CFR Part 2.

b. For Judicial and Administrative Proceedings, in response to:

i) An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or

ii) Generally speaking, although allowed by HIPAA, applicable state law bars the release of health information in response to a subpoena, discovery request or other lawful process not accompanied by a court order. If a subpoena is received for the release of health information, the Privacy Official should be notified immediately.

c. Unless state confidentiality laws dictate otherwise, to a Law Enforcement Officer for Law Enforcement Purposes, under the following conditions:

i) Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.

ii) Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.

iii) Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.

iv) Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

v) Information that constitutes evidence of criminal conduct that occurred on *Heiden Chiropractic Inc.*'s premises.

d. For disclosures related to alcohol or substance abuse records, federal law prohibits any disclosure, except in very limited circumstances, that would identify a client as an alcohol or drug abuser either directly, by reference to other publicly available information, or through verification of such identification by another person. See 42 CFR § 2.12(a)(1)(i).

e. To Appropriate Public Health Authorities for Public Health Activities.

f. To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

g. To a Coroner or Medical Examiner about Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

h. For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

i. For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

j. To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

k. For Specialized Government Functions, including disclosures of PHI of an incarcerated individual to a correctional institution and disclosures of an individual's PHI to authorized federal officers for the conduct of national security activities.

l. For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation of other similar programs.

d. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if the client provides an authorization that satisfies all of HIPAA's requirements for a valid authorization. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. *See* 45 CFR § 164.508(a).

Objective: To facilitate disclosures of PHI as permitted by HIPAA when authorized by the individual whose PHI will be disclosed. PHI disclosed pursuant to an individual authorization may be disclosed for any purpose so long as the disclosure is consistent with the terms of the authorization. *See* 45 CFR § 164.508.

1. Procedure for Disclosures of PHI Pursuant to An Authorization

a. ***Disclosure Pursuant to Individual Authorization***. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

i) Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

b. Verify that the authorization form is valid. Valid authorization forms are those that are written in plain language and:

i) Are properly signed and dated by the individual or the individual's representative;

ii) Are not expired or revoked. The expiration date of the authorization form must be a specific date or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of

the use or disclosure (e.g., for the duration of the individual's coverage);

iii) Contain a description of the information to be used or disclosed;

iv) Contain the name of the entity or person authorized to use or disclose the PHI;

v) Contain the name of the recipient of the use or disclosure;

vi) Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and

vii) Contain a statement regarding the possibility for a subsequent re-disclosure of the information. All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.

viii) Contain a statement about *Heiden Chiropractic Inc.*'s ability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.

c. Use an authorization that is in full compliance with the HIPAA privacy rule, such as the *Authorization for Release of Information Form.*

d. Provide the individual with a copy of the signed authorization.

e. Disclosures must be documented in accordance with the procedure for "Documentation and Retention." See 45 CFR § 164.508.

e. Verification of Identity of Those Requesting PHI

Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PM of his or her minor child, a personal representative, or a public officer seeing access.

Objective: To verify the identity and authority of individual requesting access to PHI.

1. Procedure for Verifying the Identify of Person Requesting PHI[63]

a. ***Request Made by Individual***. When an individual requests access to his or her own PHI, the following steps should be followed:

i) Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.

ii) Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.

iii) Make a copy of the identification provided by the individual and file it with the individual's Designated Record Set in the client's record in the Radiology Information System utilized by *Heiden Chiropractic Inc.*.

iv) Document disclosures in accordance with the procedure for "Documentation and Retention."

b. ***Request Made by Parent Seeking PHI of Minor Child***. When a parent requests access to the PHI of the parent's minor child that does not involve sensitive health information such as alcohol and drug abuse or HIV test results, the following steps should be followed:

i) Seek verification of the person's relationship with the child.

ii) Disclosures must be documented in accordance with the procedure "Documentation and Retention."

If the information request involves sensitive information such as that described above, contact the Privacy Officer before making the disclosure. *See* 45 CFR § 164.514(h); 42 CFR § 2.14.

c. ***Request Made by Personal Representative.*** When a personal representative requests access to an individual's PHI the following steps should be followed:[64]

i) Require a copy of a valid power of attorney or other documentation providing evidence of personal

[63] See 45 CFR § 164.514(h).
[64] See 45 CFR § 164.514(h).

representative status. If there are any questions about the validity of this document, seek review by the Privacy Official.

ii) Make a copy of the documentation provided and file it with the individual's Designated Record Set.

iii) Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

d. ***Request Made by Public Officer.*** If a public officer requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," the following steps should be followed to verify the officer's identity and authority:[65]

i) If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's Designated Record Set.

ii) If the request is in writing, verify that the request is on the appropriate government letterhead.

iii) If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

iv) Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Official.

v) Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

[65] See 45 CFR § 164.514(h)(2)(iii).

f. Complying With the "Minimum Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

Until the Secretary issues guidance on what constitutes "minimum necessary," the term shall mean the "limited data set" of the PHI, to the extent that disclosure of the limited data set is practicable.[66] *Heiden Chiropractic Inc.*, through its Privacy Officer, will monitor the DHHS website and/or consult other resources to learn of new guidance issued by the Secretary. Once the Secretary issues guidance, *Heiden Chiropractic Inc.* will comply with that guidance when determining what qualifies as "minimum necessary."

If the "limited data set" is not practicable for the purpose of the permitted disclosure, then *Heiden Chiropractic Inc.* shall disclose only the PHI needed to accomplish the intended purpose of such use, disclosure or request.

Objective: To limit the PHI used, disclosed or requested to the "minimum necessary" to accomplish the purpose of the use, disclosure or request unless an exception applies.

1. Exceptions to Minimum Necessary Standard[67]

    a. The "limited data set" or minimum necessary limitation shall not apply to:

        i) Disclosures to or requests by a health care provider for treatment;

        ii) Uses or disclosures made to the Individual;

        iii) Uses or disclosures made pursuant to a valid authorization under HIPAA;

        iv) Disclosures made to the Secretary pursuant to the HIPAA Security Standards;

---

[66] HIPAA defines "limited data set" as PHI that excludes the following direct identifies of the Individual or of relatives, employers, or household members of the Individual: 1) names; 2) address (other than town or city, State, and zip code); 3) telephone numbers; 4) fax numbers; 5) electronic mail addresses; 6) social security numbers; 7) medical record numbers; 8) health plan beneficiary numbers; 9) account numbers; 10) certificate/license numbers; 11) vehicle identifies and serial numbers, including license plate numbers; 12) device identifies and serial numbers; 13) web universal resource locators (URLs); 14) internet protocol (IP) address numbers; 15) biometric identifiers, including finger and voice prints; and 16) full face photographic images and any comparable images.

[67] See 45 CFR § 164.502(b) and HITECH § 13405.

v) Uses or disclosures required by law; and

vi) Uses or disclosures that are required for compliance with applicable requirements of HIPAA.[68]

b. ***Minimum Necessary When Disclosing PHI***. For making disclosures of PHI for which the minimum necessary rule applies, the disclosure must be reviewed on an individual basis by the Privacy Official or his designated staff to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure. Recurring disclosures may, in the Privacy Official's discretion, be disclosed based on a procedure established by the Privacy Official and thereby without review of each individual disclosure.

c. ***Minimum Necessary When Requesting PHI***. For making requests for disclosure of PHI from another covered entity for purposes of *Heiden Chiropractic Inc*.'s operations, only the minimum information necessary for the purpose will be requested.

2. Procedure for Disclosures Pursuant to the Minimum Necessary Standard

For any disclosure not in the above listed Exceptions to the Minimum Necessary Standard, notify the Privacy Official prior to disclosure. The Privacy Official will determine whether the PHI to be released complies with the minimum necessary rule. The Privacy Official may identify regularly recurring disclosures and identify the types of PHI to be disclosed, the types of person who may receive the PHI, and the conditions that would apply to such access for these regularly recurring disclosures.

3. Procedure for Requests for PHI Pursuant to the Minimum Necessary Standard

For any request not exempted from the minimum necessary rule, notify the Privacy Official prior to disclosure. The Privacy Official will determine whether the PHI to be released complies with the minimum necessary rule. The Privacy Official may identify regularly recurring disclosures and identify the types of PHI to be disclosed, the types of person who may receive the PHI, and the conditions that would apply to such access for these regularly recurring disclosures.[69]

---

[68] 45 CFR § 164.502(b).

[69] See 45 CFR § 164.514(d).

g. Disclosures of PHI to Business Associates

Employees may disclose PHI to *Heiden Chiropractic Inc.*'s business associates and allow *Heiden Chiropractic Inc.*'s business associates to create or receive PHI on its behalf. However, prior to doing so, *Heiden Chiropractic Inc.* must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors, employees must contact the Privacy Official and verify that a business associate contract is in place.

Definition of Business Associate: An entity or person who:[70]

- Performs or assists in performing a covered function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service *Heiden Chiropractic Inc.* access to PHI.

Objective: To verify that disclosure of PHI to business associates is consistent with a valid business associate contract.

1. Procedure for Disclosures of PHI to Business Associates

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a "business associate" must be made in accordance with a valid business associate agreement. The business associate agreement will incorporate all provisions required by 45 CFR § 164.314(a); § 164.504(e) and HITECH. See *Business Associate Agreement Form*. Before providing PHI to a business associate, employees must contact the Privacy Official and verify that a business associate agreement is in place. The following additional procedures must be satisfied:

a. Disclosures must be consistent with the terms of the business associate agreement.

b. Disclosures must comply with the "Minimum Necessary" Standard.

c. Disclosures must be documented in accordance with the procedure for "Documentation and Retention."

[70] See 45 CFR § 164.502(e)(1).

h. Disclosures of De-Identified Information

Heiden Chiropractic Inc. may freely use and disclose de-identified information. De-identified information is health information that cannot identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing eighteen (18) specific identifiers (i.e., name, social security number, etc.).

To the extent that *Heiden Chiropractic Inc.* has clients who are being treated for alcohol or other substance abuse, the disclosure must comply with 42 CFR § 2.12, which restricts the disclosure of information that would identify a patient as an alcohol or drug abuser, either directly, by reference to other publicly available information, or through verification of such an identification by another person. *See* 45 CFR §§ 514(a); 42 CFR § 2.12.

Objective: To permit disclosure of de-identified information in accordance with HIPAA.

1. Procedure for Disclosing De-identified Information[71]

    a. Obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.

    b. *Heiden Chiropractic Inc.* may freely use and disclose de-identified information. De-identified information is not PHI.

i. Requests for Disclosure of PHI from Spouses, Family Members, and Friends

Heiden Chiropractic Inc. will not disclose PHI to family and friends of an individual except as required or as permitted by HIPAA and other more stringent state and federal laws, such as 42 CFR Part 2 (relating to alcohol and substance abuse information) and Wis. Stat. §§ 51.30 and 146.82. Generally, an authorization is required before another party, including a spouse, family member or friend, will be able to access PHI.

Objective: To protect privacy of individual's PHI by disclosing it only as authorized.

1. Procedure for Handling Disclosure Requests from Family and Friends[72]

    a. If an employee receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an

[71] See 45 CFR § 164.514(a).
[72] See 45 CFR § 164.510(b).

individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual and the request is not related to sensitive health information such as alcohol and drug abuse services or HIV test results, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

b. Once the identity of a parent or personal representative is verified, then follow the procedure for "Individual's Request for Access."

c. In the case of sensitive health information requests from family members, the employee shall consult with the Privacy Officer to determine if state or federal law permits the disclosure without consent.

d. All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

j. Fundraising[73]

Heiden Chiropractic Inc. may use or disclose the following PHI to a Business Associate or institutionally-related foundation for the benefit of raising funds without a patient authorization: 1) demographic information; 2) dates of health care provided to the individual. However, *Heiden Chiropractic Inc.* shall allow individuals an opportunity to opt-out of receiving fundraising communications.

1. Procedure for Using or Disclosing PHI for Fundraising Purposes

a. *Heiden Chiropractic Inc.* shall assess whether a communication qualifies as fundraising, which is defined as raising funds for *Heiden Chiropractic Inc.*'s own benefit by communicating certain PHI to either Business Associates or institutionally-related foundations.

b. If the communication qualifies as fundraising, *Heiden Chiropractic Inc.* shall provide, without the individual's authorization, the individual's demographic information, dates that the individual received health care, department of service information, treating physician, outcome information, and health insurance status only.

c. To the extent that *Heiden Chiropractic Inc.* determines that it makes fundraising communications, it must include in its Notice of

[73] HITECH § 13406(b).

Privacy Practices a statement regarding that *Heiden Chiropractic Inc.* may contact the individual regarding fundraising.

d. *Heiden Chiropractic Inc.* shall include in all of its fundraising communications a clear description of how the individual may opt-out of receiving any further fundraising communications.

e. Any written fundraising communication that is a healthcare operation, as defined by 45 CFR § 164.501 and which includes (but is not limited to) communications about outcomes evaluation, quality assessments, population-based activities relating to improving health or reducing health care costs, shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communication to elect not to receive any further such communication.

f. In order to satisfy the notice of opt-out requirement described above, *Heiden Chiropractic Inc.* may decide to use the Fundraising Opt-Out Form and include it with each fundraising communication.

g. When an individual elects not to receive any further such communication, such election shall be treated as a revocation of a HIPAA authorization under 45 CFR § 164.508(b)(5). As a result, *Heiden Chiropractic Inc.* will not provide or involve the Individual in its fundraising communications.

h. *Heiden Chiropractic Inc.* will retain documentation related to an Individual's decision to opt-out of receiving fundraising communications for a period of not less than 6 years.

k. Marketing[74]

It is the policy of *Heiden Chiropractic Inc.* that it will communicate with Individuals about products or services only if *Heiden Chiropractic Inc.* obtains an authorization for any such use or disclosure, unless the communication is: 1) in person; 2) a refill reminder or other communication about a drug or biologic currently bein prescribed to the patient and the financial remuneration being received by *Heiden Chiropractic Inc.* in exchange for making the communication is reasonably related to *Heiden Chiropractic Inc.*'s cost of making the communication; or 3) a promotional gift of nominal value provided by *Heiden Chiropractic Inc.*.

1. Procedure for Using and Disclosing for Marketing Purposes

[74] HITECH § 13406(a).

a. In the case of communications about products or services promoted by *Heiden Chiropractic Inc.* for which *Heiden Chiropractic Inc.* receives ***no direct or indirect payment***, *Heiden Chiropractic Inc.* may make such communications to an Individual without the Individual's authorization if *Heiden Chiropractic Inc.* limits those communications to:

i) Descriptions of health-related products or services (or payment for such products or services) that are provided by, or included in a plan of benefits, including communications about: *Heiden Chiropractic Inc.* participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

ii) Information related to treatment of the Individual; or

iii) Information related to case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

b. If *Heiden Chiropractic Inc.* ***will receive direct or indirect payment*** (other than payment for treatment) for any of the communications listed above, *Heiden Chiropractic Inc.* must secure the individual's written authorization pursuant to 45 CFR § 164.508(b) and such authorization must state that such remuneration is involved.

2. Sale of Electronic Health Records or PHI[75]

It shall be the policy of *Heiden Chiropractic Inc.* that it will not disclose an Individual's PHI in exchange for remuneration unless *Heiden Chiropractic Inc.* obtains a valid authorization from the Individual in accordance with 45 CFR § 164.508 or unless one of the exceptions listed in the procedure applies. *See Sale of EHR Procedure and Sale of EHR or PHI Authorization Form.*

The authorization referenced above must specify whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual.

3. Procedure for Disclosing PHI for Remuneration

[75] HITECH § 13405(d).

Heiden Chiropractic Inc. may disclose an Individual's PHI in exchange for remuneration, without an Individual's authorization, only if any of the following apply:

a. The purpose of the exchange is for public health activities, as described in 45 CFR § 164.512(b), or is a Limited Data Set pursuant to a data use agreement as provided in 45 CFR § 164.514(e).

b. The purpose of the exchange is for research, as described in 45 CFR § 164.512(i) or 45 CFR § 164.514(e), and the price charged reflects the costs of preparation and transmittal of the data for such purpose.

c. The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access.

d. The purpose of the exchange is for the business management and general administrative activities of *Heiden Chiropractic Inc.*, including the sale, transfer, merger, or consolidation of all or part of *Heiden Chiropractic Inc.* with another Covered Entity or an entity that following such activity will become a Covered Entity and due diligence related to such activity requires such exchange.

e. The purpose of the exchange is for remuneration that is provided by *Heiden Chiropractic Inc.* to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on behalf of and at the specific request of *Heiden Chiropractic Inc.* pursuant to the Business Associate Agreement and is otherwise in compliance with federal and state laws.

f. The purpose of the exchange is to provide an Individual with a copy of the Individual's PHI pursuant to 45 CFR § 164.524.

g. The purpose of the exchange is required by law or for purposes permitted by the Privacy rule, where the only remuneration received by *Heiden Chiropractic Inc.* is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

7. Procedures for Complying with Individual Rights

This section includes procedures for complying with an individual's right to access, amendment, and accounting of disclosures of PHI held in a Designated Record Set. This section also includes procedures for addressing individual requests for confidential communications and for limits on use and disclosure.

a. Access to Protected Health Information and Requests for Amendment

HIPAA gives clients the right to access and obtain copies of their PHI that *Heiden Chiropractic Inc.* (or its Business Associates) maintains in Designated Record Sets (as defined below). It shall be the policy of *Heiden Chiropractic Inc.* to provide Individuals with electronic access to copies of their designated record set in their Electronic Health Record when possible and when required by law. HIPAA also provides that clients may request to have their PHI amended. *Heiden Chiropractic Inc.* will provide access to PHI and it will consider requests for amendment that are submitted in writing by clients.

"Designated Record Set" is defined as a group of records maintained by or for *Heiden Chiropractic Inc.* that includes:[76]

- The medical records and billing records about individuals maintained by *Heiden Chiropractic Inc.*;
- The enrollment, payment, and claims adjudication record of an individual maintained by or for *Heiden Chiropractic Inc.*; or
- Other protected health information used, in whole or in part, by or for *Heiden Chiropractic Inc.* to make coverage decisions about an individual.

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with access to their own PHI maintained in a Designated Record Set in the client's record maintained by *Heiden Chiropractic Inc.*.

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with the right to request amendments to their own PHI.

1. Procedure for Allowing PHI Access to Individuals

a. ***Request from Individual, Parent of Minor Child, or Personal Representative***. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employee must take the following steps:[77]

i) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

[76] See 45 CFR § 164.524 and 526.
[77] See 45 CFR § 164.524(a).

ii) Review the disclosure request to determine whether the PHI requested is held in the individual's Designated Record Set. See the Privacy Official if it appears that the requested information is not held in the individual's Designated Record Set. No request for access may be denied without approval from the Privacy Official.

iii) Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access:

(A) Psychotherapy notes, AODA or HIV test results;

(B) Documents compiled for a legal proceeding;

(C) Information compiled during research when the individual has agree to denial of access;

(D) Information obtained under a promise of confidentiality; or

(E) Other disclosures that are determined by a health care professional to be likely to cause harm.

iv) See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.

v) Unless state law requires a faster response time to requests for access, respond to the request for access by providing the information or denying the request within thirty (30) days (sixty (60) days if the information is maintained off site). If the requested PHI cannot be accessed within the thirty (30) day (or sixty (60) day) period, the deadline may be extended for thirty (30) days by providing written notice to the individual within the original thirty (30) day or sixty (60) day period of the reasons for the extension and the date by which *Heiden Chiropractic Inc.* will respond.

vi) A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.

vii) *Heiden Chiropractic Inc.* shall provide an individual access to their designated record set in electronic format when possible, except *Heiden Chiropractic Inc.* shall not provide the individual access to:

(A) Psychotherapy notes;

(B) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

(C) PHI maintained by *Heiden Chiropractic Inc.* that is subject to the Clinical Laboratory Improvements Amendments of 1988 to the extent the provision of access to the Individual would be prohibited by law (see 42 USC § 263a) or PHI maintained by *Heiden Chiropractic Inc.* that is exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR § 493.3(a)(2);[78]

(D) Information compiled during research when the individual has agreed to denial of access;

(E) Information obtained under a promise of confidentiality; or

(F) Other disclosures that are determined by a health care professional to be likely to cause harm.

viii) Individuals shall have the right to obtain from *Heiden Chiropractic Inc.* a copy of their designated record set in an electronic format and, if the Individual chooses, to direct *Heiden Chiropractic Inc.* to transmit such copy directly to an entity or person designated by the Individual, provided that any such choice is clear, conspicuous and specific.

ix) *Heiden Chiropractic Inc.* shall review state laws regarding electronic access to health records and determine if there are any additional requirements. See e.g., Wis. Stat. § 146.83(1k) (requiring written explanation when copies cannot be provided in electronic format).

x) Individuals who wish to access their Electronic Health Record should submit an Electronic Health Record Request Form to [Name of Covered Entity person], Privacy Officer.

[78] See 45 CFR § 164.524(a).

xi) Any fee that *Heiden Chiropractic Inc.* imposes for providing such Individual with a copy of his or her designated record set (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than *Heiden Chiropractic Inc.*'s labor costs in responding to the request for the copy (or summary or explanation), unless otherwise specified by state law.

xii) If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.

xiii) Disclosures must be documented in accordance with the procedure "Documentation Requirements."

2. Procedure for Allowing Individuals to Amend their PHI

a. ***Request from Individual, Parent of Minor Child, or Personal Representative.*** Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a Designated Record Set, the employee must take the following steps:[79]

i) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

ii) Review the disclosure request to determine whether the PHI at issue is held in the individual's Designated Record Set. See the Privacy Official if it appears that the requested information is not held in the individual's Designated Record Set. No request for amendment may be denied without approval from the Privacy Official.

iii) Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official.

[79] See 45 CFR § 164.526.

iv) Review the request for amendment to determine whether the amendment is appropriate. That is, determine whether the information in the Designated Record Set is accurate and complete without the amendment.

v) Unless state law requires a faster response time, respond to the request within sixty (60) days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the sixty (60) day period, the deadline may be extended for another thirty (30) days by providing written notice to the individual within the original sixty (60) day period of the reasons for the extension and the date by which *Heiden Chiropractic Inc.* will respond.

vi) If an amendment is accepted, make the change in the Designated Record Set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.

vii) When an amendment request is denied, the following procedures apply:

(A) All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.

(B) If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and *Heiden Chiropractic Inc.*'s rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record

to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

b. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six (6) years, except in the case of an accounting relating to disclosures to carry out treatment, payment or health care operations, in which case the accounting will cover only the three years prior to the date on which the accounting is requested. Several disclosures are not included in this accounting, such as disclosures:

- To individuals about their own PHI;
- Incident to an otherwise permitted uses or disclosures;
- Pursuant to an authorization;
- For purposes of creation of a facility directory or to persons involved in the client's care or other notification purposes;
- As part of a limited data set; and
- For other national security or law enforcement purposes.

Heiden Chiropractic Inc. shall respond to an accounting request within sixty (60) days. If *Heiden Chiropractic Inc.* is unable to provide the accounting within sixty (60) days, it may extend the period by thirty (30) days, provided that it gives the client notice (including the reason for the delay and the date the information will be provided) within the original sixty (60) day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any twelve (12) month period shall be provided free of charge. *Heiden Chiropractic Inc.* may impose reasonable production and mailing costs for subsequent accountings.

For accountings of treatment, payment or health care operations disclosures, *Heiden Chiropractic Inc.* accounting will provide only that information required by the Secretary of DHHS by rule, once such rules are available.

- With regard to disclosures by Business Associates, *Heiden Chiropractic Inc.* will decide whether to include in its accounting about treatment, payment or health care operations disclosures to the individual: 1) all disclosures made by its Business Associates; or 2) only an accounting of disclosures made by *Heiden Chiropractic Inc.* and a list of all Business Associates acting on behalf of *Heiden Chiropractic Inc.*, including contact information for each Business Associate listed so that the individual can contact the Business associate directly for such accounting.

Heiden Chiropractic Inc. shall ensure that its Business Associate Agreement reflects the appropriate responsibility for the Business Associate to respond to requests for accounting of disclosures.

Heiden Chiropractic Inc. will document the information required to be included in the accounting, as defined by guidance or rules issued by DHHS and pursuant to the Accounting of Disclosures Form and retain all documentation related to the accounting of disclosures request for a period of at least 6 years.[80]

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with the right to receive an accounting of certain disclosures of their PHI.

1. Procedure for Processing Requests for An Accounting of Disclosures of PHI

   a. ***Request from Individual, Parent of Minor Child, or Personal Representative.*** Upon receiving a request from an individual, (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:[81]

      i) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

      ii) If the individual requesting the accounting has already received one accounting within the twelve (12) month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.

[80] See 45 CFR § 164.528; HITECH § 13405(c).
[81] See 45 CFR § 164.528; HITECH § 13405(c).

iii) Respond to the request within sixty (60) days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the sixty (60) day period, the deadline may be extended for another thirty (30) days by providing written notice to the individual within the original sixty (60) day period of the reasons for the extension and the date by which *Heiden Chiropractic Inc.* will respond.

iv) The accounting must include disclosures (but not uses) of the requesting individual's PHI made by *Heiden Chiropractic Inc.* and any of its business associates during the period requested by the individual up to six (6) years prior to the request, except in the case of an accounting relating to disclosures to carry out treatment, payment or health care operations, in which case the accounting will cover only the three years prior to the date on which the accounting is requested. Several disclosures are <u>not</u> included in this accounting, such as disclosures:

(A) To individuals about their own PHI;

(B) Incident to an otherwise permitted uses or disclosures;

(C) Pursuant to an authorization;

(D) For purposes of creation of a facility directory or to persons involved in the client's care or other notification purposes;

(E) As part of a limited data set; and

(F) For other national security or law enforcement purposes.

v) *Heiden Chiropractic Inc.* shall respond to an accounting request within sixty (60) days. If *Heiden Chiropractic Inc.* is unable to provide the accounting within sixty (60) days, it may extend the period by thirty (30) days, provided that it gives the client notice (including the reason for the delay and the date the information will be provided) within the original sixty (60) day period.

vi) For accountings of treatment, payment or health care operations disclosures, *Heiden Chiropractic Inc.* accounting will provide only that information required by the Secretary of DHHS by rule, once such rules are available.

(A) With regard to disclosures by Business Associates, *Heiden Chiropractic Inc.* will decide whether to include in its accounting about treatment, payment or health care operations disclosures to the individual: 1) all disclosures made by its Business Associates; or 2) only an accounting of disclosures made by *Heiden Chiropractic Inc.* and a list of all Business Associates acting on behalf of *Heiden Chiropractic Inc.*, including contact information for each Business Associate listed so that the individual can contact the Business associate directly for such accounting.

vii) *Heiden Chiropractic Inc.* shall ensure that its Business Associate Agreement reflects the appropriate responsibility for the Business Associate to respond to requests for accounting of disclosures.

viii) The accounting must include the following information for each reportable disclosure of the individual's PHI.

(A) The date of disclosure;

(B) The name (and if known, the address) of the entity or person to whom the information was disclosed;

(C) A brief description of the PHI disclosed; and

(D) A brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)

ix) If *Heiden Chiropractic Inc.* has received a temporary suspension statement from a health oversight agency or a law enforcement officer indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official for more guidance.

x) *Heiden Chiropractic Inc.* will document the information required to be included in the accounting, as defined by guidance or rules issued by DHHS and pursuant to the *Accounting of Disclosures Form* and retain all documentation related to the accounting of disclosures request for a period of at least 6 years in accordance with the Documentation and Retention policy and procedure.

c. Requests for Alternative Communication Means or Locations

Clients may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, clients may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of *Heiden Chiropractic Inc.*, the requests are reasonable.

However, *Heiden Chiropractic Inc.* shall accommodate such a request if the client clearly provides information that the disclosure of all or part of that information could endanger the client. The Privacy Official has responsibility for administering requests for confidential communications.[82]

Objective: To facilitate processing of requests for confidential communications.

1. Procedure for Processing Requests for Confidential Communications

a. ***Request From Individual, Parent of Minor Child, or Personal Representative.*** Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:[83]

i) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

ii) Determine whether the request contains a statement that disclosure of all or some of the information to which the request pertains could endanger the individual.

iii) The employee should take steps to honor requests that are reasonable. Requests for confidential communications must be honored by *Heiden Chiropractic Inc.* if the

[82] See 45 CFR § 164.522(b).
[83] *See* 45 CFR § 164.522(b).

individual states that disclosure could endanger the individual.

iv) If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

v) All confidential communication requests that are approved must be tracked by the Privacy Official to ensure compliance.

vi) Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

d. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A client may request restrictions on the use and disclosure of the client's PHI. It is *Heiden Chiropractic Inc.*'s policy to attempt to honor such requests if, in the sole discretion of *Heiden Chiropractic Inc.*, the requests are reasonable. However, *Heiden Chiropractic Inc.* will honor the request in all cases involving disclosures to a health plan for purposes of carrying out payment or health care operations, when that disclosure:

- Pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full; and
- Is not otherwise required by law.

Heiden Chiropractic Inc. shall require Individuals who request such restrictions on disclosures of their PHI to submit *Heiden Chiropractic Inc.*'s *Mandatory Restrictions on Disclosures Form*.

Heiden Chiropractic Inc. shall retain documents related to an Individual's request to restrict disclosures for a period of at least 6 years. *See* 45 CFR 164.522(a); HITECH § 13405(a).

Objective: To facilitate the processing of requests for restrictions on uses and disclosures of PHI.

1. Procedure for Processing Requests for Restrictions on Uses and Disclosures of PHI

a. ***Request From Individual, Parent of Minor Child or Personal Representative.*** Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for

restrict any otherwise permitted use or disclosure of an individual's PHI, the employee must take the following steps:[84]

i) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

ii) The employee should take steps to honor requests that are reasonable except that *Heiden Chiropractic Inc.* shall honor the request in all cases involving disclosures to a health plan for purposes of carrying out payment or health care operations, when that disclosure:

(A) Pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full; and

(B) Is not otherwise required by law.

Heiden Chiropractic Inc. shall require Individuals who request such restrictions on disclosures of their PHI to submit *Heiden Chiropractic Inc.*'s *Mandatory Restrictions on Disclosures Form*.

Heiden Chiropractic Inc. shall retain documents related to an Individual's request to restrict disclosures for a period of at least 6 years. *See* 45 CFR 164.522(a); HITECH § 13405(a).

Heiden Chiropractic Inc. will honor all other requests that will not unduly impede the ability of *Heiden Chiropractic Inc.* to fulfill its legal obligations.

iii) If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

iv) All requests for limitations on use or disclosure of PHI that are approved must be tracked by the Privacy Official to ensure compliance.

[84] See 45 CFR § 164.522(a); HITECH § 13405(a).

v) All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions by the Privacy Official.

vi) Requests and their dispositions must be documented in accordance with the procedure for "Documentation and Retention."