Purpose

To ensure the patient's/client's right to privacy and security as well as respect for the patient's/client's property is observed.

Definition

I. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule – Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient/client authorization. The Rule also gives patients'/clients' rights over personal health information, including rights to examine and obtain a copy of personal health records, and to request corrections.

II. HIPAA Security Rule – Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

III. HIPAA Breach Notification Rule – Requires HIPAA covered entities and business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and third-party service providers, pursuant to Section 13407 of the HITECH Act of 2009.

Policy

I. The Agency will give the Notice of Privacy Practices to the Governing Body, all staff involved in patient/client care, potential employees, healthcare students, consultants, and business associates which explains the patient's/client's rights regarding confidentiality, privacy, and security.

II. The Agency will give and explain to the patient/client, the representative (if any), and the caregiver the Notice of Privacy Practices regarding privacy rights as mandated by the Privacy Rules of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its revisions, as applicable.

III. The Agency will comply with all applicable HIPAA Security Rules, to include all of the patients'/clients' electronic protected health information (ePHI).

IV. The Agency and agent acting on behalf of the Agency in accordance with a written contract must ensure the confidentiality of all patient/client identifiable information contained in the clinical

record, including OASIS data, and may not release patient/client identifiable OASIS information to the public.

V. The Agency will inform the patient/client, the representative (if any), or the caregiver both verbally and in writing upon admission, regarding the Statement of Patient Privacy Rights and the Privacy Act Statement-Health Care Records pertaining to OASIS data. The Agency will obtain acknowledgment of patient/client receipt.

VI. The Governing Body will be informed of and sign a "Confidentiality/Conflict of Interest Disclosure Statement".

VII. The patient/client, the representative (if any), and the caregiver will be informed upon admission regarding confidentiality.

VIII. The patient's/client's property will be respected during the provision of patient/client care.

Procedure

I. HIPAA Privacy Rules

A. Clinical

1. The Agency will provide all current employees with training on the HIPAA Rules, including Privacy, Security, and Breach Notification.
2. All new employees will receive HIPAA training during orientation.
3. If the Agency changes its policies and procedures, all employees will receive retraining.
4. All HIPAA orientation and retraining will be documented in the employees' personnel files.
    a. The Privacy Officer will maintain a record of Privacy, Security, and Breach Notification training given to the employees as defined in the HIPAA Privacy, Security, and Breach Notification Rules.
5. Upon admission, patients/clients, the representatives (if any), and the caregivers will be informed both verbally and in writing regarding confidentiality, as well as access to, release of, and the safeguarding of patient/client records as delineated in the Notice of Privacy Practices.
    a. This information includes, but is not limited to:
        (1) Request to restrict use and disclosure of protected health information (PHI)
        (2) Request to receive confidential communications
        (3) Request to access PHI

(4) Request to amend PHI

(5) Request for disclosure of PHI

(6) Right to be notified following a breach of unsecured PHI

b. The need for authorizations to release information to individuals not covered by HIPAA will be explained.

c. The patient/client will be instructed to contact the Privacy Officer.

d. The patient/client will be assured that the Agency will:

(1) Restrict employees' access to the minimum amount of PHI necessary to perform job

(2) Disclose only the minimum amount of data necessary per the requested purpose

(3) Request only the minimum amount of PHI needed from other covered entities

e. The patient/client will be informed of the option to opt out of receiving fundraising information per the Notice of Privacy Practices.

f. The patient/client will be informed of the option to opt out of receiving marketing information per the Notice of Privacy Practices.

6. Agency staff will obtain a consent to obtain photographs of the patient/client and/or patient's/client's wounds prior to taking the photograph.

B. Business

1. The Agency restricts the use and disclosure of certain types of information that could be advantageous to other businesses or harmful to the Agency, its patients/clients, or its employees.

2. Confidential business information is considered the agency's property.

3. Utilization of confidential information for personal gain is considered by the Agency to be improper and/or unlawful.

4. Discussion of confidential information with family, friends, or business and professional associates should be avoided.

5. Employees will be educated regarding confidentiality pertaining to use of an electronic record, Point of Care devices, computers, electronic devices and media, information kept in the car, discussions of one patient/client to another, and other aspects of potential breach of confidentiality. Employee education regarding confidentiality will include, as appropriate, the utilization of smartphones, wireless access points (WAPs), memory cards,

disks, CDs, DVDs, backup media, smart cards, and remote access devices (including security hardware).

6. Employee data/information requested upon hire, and periodically thereafter, is required for and considered pertinent to the agency's business.

7. Employees and Governing Body members have a responsibility to have no conflicting interest when representing the Agency in negotiations or making recommendations about a third-party. The employees and Governing Body members will work with patients/clients, caregivers, and other parties doing business with the Agency on the basis of what is in the agency's best interest without showing favor or preference to third parties based on personal considerations.

8. An employee or Governing Body member who deals with third parties on behalf of the Agency, or who makes recommendations or approvals or rejections, will not own any interest in or have any personal contact with the third-party that could possibly influence the employee in regard to the best interest of the Agency.

9. An employee or member of the Governing Body will not directly or indirectly seek or accept payments, loans, services, excessive entertainment, travel, gifts, or other reward from any individual or representative of any business or individual seeking to do business with the Agency that might tend to influence the decision of the employee with respect to the agency's business.

C. Business Associates

1. The agency's business associates will have access to the minimum amount of patient/client PHI needed to accomplish the cited purpose (see the Professional Services Contract).

II. HIPAA Security Rules

A. The Agency will appoint an Information Security Officer to oversee compliance with the HIPAA Security Rules.

1. This individual may be the Privacy Officer.

B. The Agency will provide security and awareness training to all employees, including management, upon hire and periodically thereafter.

C. The Agency will perform an initial risk assessment of ePHI to ensure the agency's security measures allow for reasonable and appropriate compliance with the HIPAA Security Rule.

1. In deciding if the security measures are adequate, the Agency may consider the following:

a. The size, complexity, and capabilities

b. The technical infrastructure, hardware, and software security capabilities

c. The costs of the security measures

d. The probability and criticality of potential risks to ePHI

2. The Agency will perform follow-up ePHI risk assessments at least annually and after any event that compromises the agency's electronic security.

D. The Agency will ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits.

E. The Agency will protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.

F. The Agency will protect against any reasonably anticipated uses or disclosures of ePHI other than those that are permitted by the HIPAA Security Rule.

G. The Agency will obtain assurances in a written contract from its business associate(s) that creates, receives, maintains, or transmits ePHI on the agency's behalf that the business associate will safeguard the information.

H. The Agency will ensure compliance with the HIPAA Security Rule by all employees, including management and business associate(s).

1. The Agency will institute sanctions against any employee as defined in its Progressive Discipline Policy up to and including termination.

2. The Agency will terminate the contract with the business associate(s) if it is determined there has been a violation of the HIPAA Security Rule.

I. The Agency will maintain the policies and procedures implemented to comply with the HIPAA Security Rule in written or electronic form.

1. The Agency will document any action or activity taken and all risk assessments made as required by the HIPAA Security Rule.

2. The Agency will make documentation available to those responsible for implementing the procedures recorded and to appropriate regulatory entities.

3. The Agency will review the documentation periodically and update it as needed in response to environmental or operational changes affecting the security of the patients'/clients' ePHI.

4. The Agency will retain the required documentation for six years from its creation or the date when it was last in effect, whichever is later.

III. Breach Notification for Unsecured Protected Health Information (PHI)

A. A breach occurs when protected health information is acquired, accessed, used, or disclosed in a way that compromises the protected health information.

B. The patient/client will be notified within 60 calendar days from discovery when a breach of protected health information occurs. The breach notification must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2. A description of the types of unsecured protected health information that were involved in the breach (such as, whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what the Agency is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, website, or postal address.

C. The Agency must send written notification:

1. To patients/clients via first-class mail at last known address, or electronically when patients/clients have agreed to this form of communication.

2. If patients/clients are deceased, notification should be mailed to the patients'/clients' next of kin or personal representatives.

3. In an emergency situation in which imminent misuse of the protected health information may occur, the Agency may notify individuals by telephone or other means, in addition to providing written notice.

4. If written notice is impossible to provide due to incomplete or outdated contact information, a substitute form of notice must be provided. When there is insufficient contact information for fewer than 10 individuals, notice may be given by telephone, another type of written communication, or other means. When sufficient contact information is unavailable for 10 or more individuals, such notice will:

a. Be in the form a conspicuous posting for a period of 90 days on the home page of the website of the Agency

b. Or be a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

c. Additionally, must include a toll-free telephone number that remains active for at least 90 days that individuals can use to learn whether personal unsecured protected health information may be included in the breach.

D. The Agency also has a duty to notify the media of a breach affecting more than 500 individuals residing in one state or jurisdiction. In this situation, the Agency must notify "prominent media outlets" serving the particular state or jurisdiction. Notice must be in written form and given no later than 60 days after discovery of the breach.

E. The Secretary of the US Department of Health & Human Services (HHS) must also receive notice of breaches.

1. When 500 or more patients/clients are involved, the Agency must mail written notification to the Secretary at the same time as it is sent to the individuals affected.

2. For breaches involving fewer than 500 patients/clients, providers must maintain documentation of these breaches throughout the year. This documentation must be sent to the Secretary no later than 60 days after the end of the calendar year.

Reference

Code of Federal Regulations, Title 42, Part 484
§484.40
§484.50(c)
§484.110(d)

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Public Law 104-191
§261 – §264

Code of Federal Regulations, Title 45, Part 160 and Subparts A and E of Part 164 – Privacy Rule

Code of Federal Regulations, Title 45, Part 160 and Part 164 – HIPAA Security Rule

Code of Federal Regulations, Title 45, Part 164
§§164.400-414 – HIPAA Breach Notification Rule

United States Code (USC), Title 42, 17937 (HITECH Act of 2009)
§13407