HIPAA
Health Insurance Portability and Accountability Act

1. HIPAA...........................................................................HI: 1
   A. Overview.................................................................HI: 1
   B. Who should comply with HIPAA?.........................HI: 1
   C. What is PHI?..........................................................HI: 2
   D. The Privacy Rule.....................................................HI: 4
   E. The Security Rule....................................................HI: 4
   F. How can I protect PHI?............................................HI: 5
   G. PHI Access & Disclosure........................................HI: 5
   H. Who are Business Associates.................................HI: 6
   I. Security Rule Expanded..........................................HI: 6
   J. Electronic Health Records (EHR) and e-PHI.............HI: 7
   K. What is a Breach in PHI?..........................................HI: 7
   L. Penalties for Violations...........................................HI: 8
   M. Recommendations for Caregivers.........................HI: 9
2. HITECH Act.................................................................HI: 10
   A. What is the HITECH Act?.........................................HI: 10
   B. What is an EHR (Electronic Health Record)?............HI: 10
   C. Impact of HITECH Act on Caregiver......................HI: 10

Bibliography.................................................................HI: 11

© Copyright Clinical Assessments by Prophecy, a Division of Prophecy Healthcare, Inc.
1. HIPAA

A. Overview

Healthcare workers and organizations rely heavily on the sharing of patient information. As we continue the transition toward electronic sharing of patient health information, healthcare workers and organizations understand that standards and technology must stay current to enable fast, secure and accurate transmission of that information across the care continuum.

As technology advances and patient information becomes more portable (easy to share), it becomes more difficult to protect the privacy of patient health information. Therefore healthcare workers, organizations, and consumers are increasingly concerned about patient privacy.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, was enacted to address these issues. HIPAA Standards establish a format for the fast and accurate exchange of health information data, and for maintaining the security of that information. The Department of Health and Human Services published two rules under HIPAA, the Privacy rule and the Security rule.

B. Who should comply with HIPAA?

All Covered Entities must comply with the HIPAA Privacy & Security Rules. A Covered Entity includes:

- Healthcare provider who transmits data electronically (i.e.: doctors, hospitals, dentists, nursing homes and pharmacies).

  ***Under HIPAA, a healthcare provider is defined as any person or organization that furnishes, bills or is paid for health care services in the normal course of business and electronically transmits and stores that healthcare information. A healthcare provider can also include a person or organization that engages a third party to process, transmit and store their claims electronically.

- Health Plans

- Healthcare Clearinghouses
C. What is PHI?

As mentioned earlier, Protected Health Information or PHI is individually identifiable health information or information that is linked to a patient. PHI concerns the health status, treatment, or payment of a specific patient that is created or received and maintained by a covered entity.

PHI does not include individually identifiable health information contained in education records and in employment records held by a covered entity serving its role as an employer.

Individually identifiable health information is health information that specifically identifies the individual, or is information that could reasonably be expected to identify an individual, even if the individual is not named.

One Example of PHI:

Mary Smith is the only 50-year-old patient with a diagnosis of lung cancer at XYZ Hospital.

The following statement DOES NOT provide individually identifiable health information about Mary Smith and is therefore NOT PHI:

- There are presently 7 persons with a diagnosis of lung cancer at XYZ Hospital.

The following statement DOES provide individually identifiable health information:

- There is a 50-year-old woman with lung cancer at XYZ Hospital.

Though the second statement does not mention Mary Smith by name, it is PHI because Mary Smith is the only person who fits the description.

Many different types of information could be used to identify an individual's PHI under the Privacy Regulations, including but not limited to:

- Patient’s name
- Patient’s address
- Any elements of dates that are directly related to an individual, including birth date, admission date, discharge date, death date
- Telephone numbers, Fax numbers, Email addresses
- Social security numbers, Medical record numbers, Account numbers
- The individual's e-mail, URL, or ISP address
- Health plan beneficiary numbers (Insurance Numbers)
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full-face photographs and any comparable images
- Any other unique identifying number, characteristic, or code

Information that meets the de-identified criteria would not be subject to the HIPAA Privacy Rule, as it would not qualify as PHI.

**How should PHI be used and disclosed?**

The HIPAA Privacy Rule allows the use or disclosure of PHI:

- For treatment
- For payment
- For health care operations
- With authorization by the individual
- When required by law

The HIPAA Privacy Rule protects the privacy of patient information. Any employee of a covered entity who is involved in the gathering, storing, and transmission of patient information MUST comply with the HIPAA Privacy Rule. Failure to follow HIPAA regulations could result in punitive fines for healthcare providers and/or individuals involved.

Protected Health Information (PHI) can be used and disclosed without a signed or verbal authorization from the patient when it is a necessary part of treatment, payment, or healthcare operations.

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.

The minimum necessary standard does NOT apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes (i.e. communication hand-offs).
- Disclosures to the individual who is the subject of the information (i.e. patient).
- Uses or disclosures made with a patient’s authorization.
- Uses or disclosures required for compliance with HIPAA Rules.
- Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.
The Minimum Necessary Rule requires that only the information needed to get the job done be provided. Healthcare organizations must obtain express permission or authorization from a patient for the purpose of marketing, advertising and other purposes. Healthcare organizations must establish written privacy policies and procedures regarding protected health information. Caregivers should refer to their hospitals health information policies and procedures regarding the use and disclosure of PHI.

D. The Privacy Rule

Under HIPAA, the Privacy Rule protects the privacy of all Protected Health Information (PHI). PHI is individually identifiable health information that is gathered, stored, or transmitted on paper, orally, or by electronic or any other media.

In general, HIPAA Privacy Rule requirements:

- Apply to most health care providers;
- Set a federal floor for protecting individually identifiable health information across all mediums (electronic, paper, and oral);
- Limit how covered entities may use and disclose individually identifiable health information they receive or create;
- Give individuals rights with respect to their PHI, including a right to examine and obtain a copy of information in their medical records and the right to ask covered entities to amend their medical record if information is inaccurate or incomplete;
- Impose administrative requirements for covered entities; and establish civil penalties.

Under the HIPAA Privacy Rule:

- All patients MUST receive a healthcare organization’s Notice of Privacy Practices.
- Patients may give a verbal authorization to provide PHI to family members and friends.
- Patients are notified of their rights to complain about an organization’s compliance with the Privacy Rule.
- Patients have the right to access and amend their own Personal Health Information

For additional information regarding the de-identification standards, see: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/guidance.html#rationale

E. The Security Rule

The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Office of Civil Rights, in conjunction with the Department of Justice, is responsible for enforcement actions resulting in criminal penalties of imprisonment and fines for HIPAA violations involving Protected Health Information (PHI).
F. How can I protect PHI?

In order to understand how a caregiver can protect PHI, it is important to understanding how PHI can be compromised.

Some Examples of ways PHI is potentially compromised:

- Conversations via Face-to-face
- Conversations via Telephone or Dictation
- Hard Drives (unprotected) i.e.: Computers, Photo Copy Machines
- Fax Transmissions
- Mobile Devices i.e.: Laptop, Mobile devices, Flash drives, CD-Rom
- Cell Phones, PDA’s
- E-mail/Text Messages
- Disposal of PHI in trash
- Unsecured PHI i.e.: No Data Encryption, Unsecured Networks, and File Cabinets
- Inappropriate access to PHI i.e.: a caregiver accessing PHI on a patient they are not caring for

For example, a caregiver who is talking on a mobile device such as a cell phone regarding a patient should be in a private location where PHI cannot be compromised. Any healthcare provider handling PHI should view themselves as responsible for the privacy and security of health information in any organization.

G. PHI Access & Disclosure

Patients have the right to access their own Protected Health Information. Patients have the right to access PHI, including electronic PHI, inspect and receive a copy of their PHI in electronic form and format. The Covered Entity must respond to the individual’s request within 30 days. An exception of this would be psychotherapy notes and information that has been gathered in anticipation of civil, criminal, or administrative action.

Patients have the right to amend their Protected Health Information. Healthcare providers should consult their organizations policies and procedures regarding the disclosing of PHI for purposes other than treatment, payment and healthcare operations.

Patients can request that the organization change any PHI that it maintains in record sets. The organization can require that these requests for change be in writing and that the individual explain the reason for the change. Individuals also have a right to have an account of access to their PHI. Individuals have a right to know the identities of those persons or agencies that have accessed their PHI for 6 years PRIOR to the request, including Business Associates.
Special Circumstances

Protecting public health, including through public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, and other public health activities, often requires access to or the reporting of the protected health information of individuals.

The Privacy Rule permits covered entities to disclose protected health information without authorization for specified public health purposes. There may be more rigorous state laws regarding special circumstances, therefore it is important for healthcare providers to be knowledgeable of policies and procedures in place for the organization they are presently working for.

H. Who are Business Associates?

In 2013, the new HIPAA rules expanded to include Business Associates of Covered Entities. A "Business Associate" includes any person or organization that functions on behalf of a covered entity that involves use or disclosure of identifiable health information. Examples of this would include billing, coding or an Electronic Health Record (EHR) Vendor. A member of the covered entity (i.e.: hospital) workforce is NOT a business associate. While a member of the hospitals workforce is not a business associate, they are required to follow all requirements under HIPAA.

I. Security Rule Expanded

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (e-PHI).

Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk (CD, DVD, Blu-ray), or digital memory card.

Transmission media used to exchange information already in electronic storage media includes the following:

- Internet
- Extranet
- Intranet
- Leased lines
- Dial-up lines
- Private networks
- Physical movement of removable/transportable electronic storage media
Certain transmissions, including paper, facsimile (fax), voice, and telephone, are NOT considered to be transmissions via electronic media under the Security Rule, since the information being exchanged did not exist in electronic form immediately before the transmission. However, paper, facsimile and telephones (including cell phones) containing PHI would be subject to the HIPAA rule.

An example of this:

- Telephone calls over standard phone lines would not be considered electronic media.
  ***Recordings of telephone calls or messages that are transmitted electronically would be considered electronic media.
- Faxed documents over standard phone lines would not be considered electronic media unless the faxed documents are uploaded electronically, such as a computer.

**J. Electronic Health Records (EHR) and e-PHI**

An EHR (Electronic Health Record) creates new responsibilities for healthcare providers to safeguard patients’ health information in electronic form. The HIPAA Security Rule establishes national standards to protect individuals’ electronic protected health information (e-PHI) that is created, received, used, or maintained by a HIPAA covered entity. Even with proper safeguards in place, Electronic Patient Health Information can be at risk for common security gaps such as cyber attack and data loss.

The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of e-PHI.

The HIPAA Security Rule does require covered providers to implement security measures, which help protect patients’ privacy by creating the conditions for patient health information to be available but not be improperly used or disclosed.

**K. What is a Breach in PHI?**

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

The HIPAA Breach Notification Rule requires covered entities to promptly notify individuals and the Secretary of the HHS of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI. There are some exceptions to Breach Rule therefore; it is critical that a healthcare provider refer to their organizations policies and procedures regarding any known/potential data breach.
Furthermore, it is critical that healthcare providers report any knowledge of potential/actual breaches immediately to their supervisor. Healthcare organizations should have contingency plans in place in order to address an actual or attempted security incident. This would include e-PHI and any electronic media containing the e-PHI, whether on or off hospital premises.

**L. Penalties for Violations**

A caregiver who works for a covered entity, such as a hospital, must abide by the organizations health information privacy and security policies and procedures mandated under HIPAA. A caregiver who violates an organizations privacy and security policies could place themselves and the organization they work for at risk for investigative or enforcement actions by HHS Office of Civil Rights. Furthermore, there may be potential violations in accordance to their respective state and professional licensing boards.

Failure to comply with the HIPAA Rules can also result in civil and criminal penalties:

**Civil Penalties**

- The U.S. Department of Health and Human Services’ Office for Civil Rights (OCR) is responsible for administering and enforcing the HIPAA Privacy and Security Rules and conducts associated complaint investigations, compliance reviews, and audits. The OCR may impose fines on covered providers for failure to comply with the HIPAA Rules.
- State Attorneys General may also enforce provisions of the HIPAA Rules.

The penalties for HIPAA violations are displayed in the following tables:

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Per Violation(Minimum)</th>
<th>Maximum Civil Money Penalties for Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know - (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause (not due to willful neglect)</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected(within required time period)</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect (not corrected)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
### Criminal Penalties for HIPAA violations

<table>
<thead>
<tr>
<th>Violations for Non-Compliance</th>
<th>Criminal Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* Up to $50,000 and 1 year in prison for improperly obtained or disclosed PHI</td>
</tr>
<tr>
<td></td>
<td>* Up to $100,000 and up to 5 years in prison for offenses committed in obtaining PHI under false pretenses</td>
</tr>
<tr>
<td></td>
<td>* Up to $250,000 and up to 10 years in prison for offenses committed in disclosing PHI with the intent to sell, transfer, or use this information for commercial advantage, personal gain, or malicious harm</td>
</tr>
</tbody>
</table>

### M. Recommendations for Caregivers

- Ensure conversations (i.e.: hand-off communications) regarding patients are done in a confidential area
  - Avoid discussing a patient's condition in front of other patients, visitors, or family members in a hallway
  - Lowering voice when discussing patient information in person and/or over the phone
  - Avoid having conversations about patients in public places, such as elevators, public hallways, or the cafeteria
- Ensure that patient-related information is not visible to public i.e.: Computer Screens
- Sign off of computers when not in use
- Use passwords on desktop and portable media devices
- Change passwords, as often as organization policy allows
- NEVER share your password
- Ensure data encrypted computers are used when handling PHI
- Keep protected health information secure i.e.: password protected, lock filing cabinets/rooms
- Use precautions to protect PHI from accidental disclosure:
  - Avoid sending PHI by e-mail if at all possible.
  - Use a fax cover sheet when faxing PHI and double check the fax number to be sure it is correct

The key is balancing the objectives of safeguarding confidentiality while engaging in communications to ensure the delivery of quality health care in an effective manner. Any individual working for a covered entity (i.e.: hospital) who may come into contact with PHI must be aware of the hospitals policies and procedures regarding HIPAA, procedures for reporting and documenting incidents or possible breaches of PHI.
2. HITECH Act

In addition to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, a new piece of legislation was ratified in 2009. The new Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) was enacted as part of the American Recovery and Reinvestment Act of 2009.

A. What is the HITECH Act?

The HITECH Act is an amendment to the previous HIPAA enforcement with an increased responsibility for the protection of PHI (Protected Health Information). The HITECH Act addresses the privacy and security concerns of electronically transmitted health information (HIPAA Administrative Simplification, 2009). A portion of the money approved in this legislation is intended for use in the expansion of Electronic Health Records (EHR) by physicians and hospitals.

B. What is an EHR (Electronic Health Record)?

An Electronic Health Record (EHR) is an electronic version of a patient’s medical history and is maintained by the provider. The electronic health record is a means to automate access to personal health information and improve clinical workflow processes. The EHR may include clinical data such as: demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports (CMS, 2010).

C. Impact of HITECH Act on Caregiver

It is essential for the healthcare provider to understand what the HITECH Act is but also how it affects you in the workplace setting.

How this new federal legislation impacts you:

- Increased development and use of EHR(Electronic Health Records) in the workplace
- Increased development and monitoring of EHR security in the workplace; in other words, who is accessing EHR and do they have a ‘need to know’
- Immediate reporting of any and all EHR security breaches
- Increased penalties for those discovered breaching safeguards contained in the Security Rules
- Requires HHS(Health and Human Services) to conduct periodic audits
- Mandatory penalties imposed for “willful neglect”

As with all Protected Health Information, it is critical for the caregiver to exercise prudence when accessing, managing, and/or transmitting any and all PHI.

The caregiver needs to know the policies of their organization regarding electronic health information and security measures that are in place to ensure security of PHI.
Bibliography


