The Holman Group
Managed Behavioral Health Care Services

HIPAA and Information Security Guidance for Providers

August 21, 2020

The Health Insurance Portability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information. You play a vital role in protecting the privacy and security of patient information.

This document contains guidance and helpful hyperlinks to assist your organization in meeting HIPAA compliance standards.

HIPAA and Information Security Guidance for Providers

August 21, 2020

What is HIPAA?

Protected Health Information (PHI) is individually identifiable health information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and that:

- May exist in hard-copy or as electronic data (ePHI)
- Relates to the past, present, or future physical or mental health or condition of an individual
- Relates to the provision of health care to an individual
- The past, present or future payment for the provision of health care to an individual

PHI is also in the hands of Business Associates. These are persons or organizations that, on behalf of a covered entity, health plan or provider:

- Perform any function or activity covered by HIPAA
- Provide a service on behalf of a covered entity involving the transfer of PHI.

What Does PHI Include?

Information in the **health record**, such as:

- Lab results
- Therapy session details
- Appointment dates/times
- Patient Identifiers
- Invoices
- Radiology films and reports
- History and physicals (H&Ps)

Who or What Protects PHI?

- **Federal Government** protects PHI through HIPAA regulations
- **Your Organization**, by implementing secure processes and data protection controls
- **Your Staff and Business Associates,** by following our policies and procedures.

Why is Training Necessary?

There are a number of reasons why security/ privacy training is necessary:

- Ensure understanding of Privacy and Security Rules.
- Fulfill Compliance Requirement.
- Communicate ways to prevent accidental and intentional misuse of PHI.
- Commitment to managing electronic protected health information (ePHI) with the same care.

Examples of Personal Identifiers:

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

HITECH Act

In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule, "the Omnibus Rule", implementing HITECH's statutory amendments to HIPAA.

Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Information Security

Information security involves the preservation of:

- **Confidentiality:** Ensuring information is only disclosed to, and reviewed exclusively by intended recipients / authorized individuals.
- **Integrity:** Ensuring the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that information and associated assets are accessible, whenever necessary, by authorized individuals.
- **Privacy:** Maintaining the right of an individual to keep his or her health information private.

HIPAA Privacy Rule

The HIPAA Privacy Rule provides federal protections for personal health information held by companies that store and manage PHI/ePHI and gives patients an array of rights with respect to that information, including:

- Get a copy of their medical records
- Ask for changes to their medical records
- Find out and limit how their PHI may be used
- Know who has received their PHI
- Have communications sent to an alternate location or by an alternate means
- File complaints and participate in investigations
- At the same time, it permits the disclosure of personal health information needed for patient care and other important purposes.

Unintentional Violations	Intentional Violations
Inadvertent, unintentional or negligent act which may or may not result in PHI being disclosed. Common occurrences include: • Faxed a Document to Wrong Location • Entered Incorrect Medical Record Number • Forgot to Verify Patient Identity • Lost a laptop that contained unencrypted ePHI	Intentional act which violates the organization's policies pertaining to that PHI which may or may not result in actual harm to the patient or personal gain to the employee. • Medical identity theft • Sale of personal information on Dark Web • Disclosure of information to journalist / media

Types Security Threats:

- Hacking (unauthorized intrusion)
- Malware (viruses, trojans, etc.)
- Surveillance (spyware)
- Denial of Service Attacks
- Ransomware
- Social Engineering
- Physical Access
- Privilege Escalation
- Phishing
- Data Leakage
- Data Breach
- Data Loss
- Espionage
- Criminal activities
- Disgruntled employees
- Natural disasters

Common Controls: Prevent and Detect

- User Access Controls
- Change and Configuration Management
- Backup and Recovery
- Disaster Recovery Planning
- Business Continuity Planning
- Incident Management
- Vulnerability Management
- Encryption
- Manage Detection Services
- Penetration Testing
- Firewalls
- IDS/IPS
- SIEM (Event Log Monitoring)
- Anti-Malware
- Web-filtering
- Deception
- Physical Security
- Training

The HIPAA Privacy Rule establishes standards to protect PHI/ ePHI held by entities and their business associates including health care providers that conduct certain health care transactions electronically and health care clearinghouses.

HIPAA Security Rule

The HIPAA Security Rule specifies safeguards for covered entities to use to assure the confidentiality, integrity, and availability of PHI/ePHI and is designed to keep secure the transfer and storage of PHI/ePHI by enforcing:

- **Administrative Procedures:** These measures manage the selection, development, implementation and maintenance of security measures and include workforce security, security training, policies and procedures.
- **Technical Safeguards:** The technology that protects PHI/ePHI and controls access and transmission security.
- **Physical Safeguards:** Physical measures to protect the electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Confidentiality: PHI/ePHI is not available or disclosed to unauthorized persons or processes.

Integrity: PHI/ePHI is not altered or destroyed in an unauthorized manner.

Availability: PHI/ ePHI is accessible and usable on demand by authorized persons.

The Privacy Rule protects PHI/ ePHI held or transmitted information by a covered entity or its business associates, in any form:


Electronic


Spoken


Paper

Visit the HHS HIPAA Guidance webpage for guidance on:

- **De-identifying PHI to meet HIPAA Privacy Rule requirements,**
- **Individuals' rights to access health information**
- **Permitted uses and disclosures of PHI**

Release of Information

When releasing PHI, it is important to know when a patient's authorization is required. In most cases, a formally documented request must be presented prior to releasing PHI. Patient authorizations are governed by state and federal law.

Prior to making any verbal disclosures of PHI, you must verify the requestor's identity by asking several identifying questions (i.e., address, birth date, member number, etc).

- Protected health information may be given to custodial parents, emancipated minors, Designated Representatives and Designated Agents as long as an authorization and/or legal documents are on file.
- Federal law protects all information about a member with a current or past diagnosis of substance abuse and/or mental disorder.

Exceptions:

You may disclose information without a member's authorization to the appropriate authorities:

- If required by law, court order, etc.
- To public health officials, FDA, CDC, etc.
- For abuse or domestic violence
- To help law enforcement officials
- To notify of suspicious death
- To provide information for workers' compensation
- To assist government actions
- To help in disaster relief efforts
- To avert a serious threat to health or safety
- For health oversight activities

HIPAA violations are enforced by the Department of Health and Human Services (HHS), however pursuant to HITECH, state attorney generals are also permitted to bring civil actions and recover monetary awards that may be shared with harmed individuals.

Reporting Security Incidents and Breaches

Definition of Breach (45 C.F.R. 164.402)

Impermissible use or disclosure of (unsecured) PHI is assumed to be a breach unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised based on a **risk assessment**.

Nature and Extent	Disclosure	Data	Mitigation
The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.	The unauthorized person who used the PHI or to whom the disclosure was made.	Determination if the PHI was acquired or viewed.	The extent to which the risk to the PHI has been mitigated.

Reporting Requirements

The **Breach Notification Rule** requires covered entities to notify affected individuals; U.S. Department of Health and Human Services (HHS); and, in some cases, the media of a breach of unsecured PHI.

Breach notifications, security, and privacy incidents must be reported to The Holman Group in writing without unreasonable delay and not later than **5-days following the discovery of a potential or confirmed incident**.

Email: compliance@holmangroup.com

Mail: Attention – Compliance Department
P.O. Box 8011, Canoga Park, CA 91309

Phone: 800-321-2843

Report incidents if you become aware or suspect any of the following:

- Potential exposure of PHI/ePHI
- Theft of or damage to equipment
- Unauthorized use of user passwords
- Unauthorized access to company networks and systems
- Excessive access to applications
- IT security policy violations
- Any other problems or questions with information security or privacy
- Lost, stolen or improperly disposed of materials containing PHI

For more information, visit the HHS Breach Notification Rule webpage for guidance on;

- Administrative requirements and burden of proof
- How to make unsecured PHI usable, unreadable, or indecipherable to unauthorized individuals
- Reporting requirements

Fraud, Waste, and Abuse

Medi-Cal / Medicaid Fraud

- Medi-Cal / Medicaid fraud involves making false statements or misrepresenting facts to obtain a benefit or payment that would not otherwise exist. These acts may be committed either for a person's own benefit or for the benefit of some other party.
- Examples include:
  - Billing for services and/or supplies that you know were not furnished or provided
  - Altering claims forms and/or receipts to receive a higher payment amount
- It is a crime to defraud the government and its programs.
- Punishment may involve imprisonment, significant fines, or both.
- Fraud may also result in civil liability and suspension from Medi-Cal Medicaid programs.

Medi-Cal / Medicaid Abuse

- Any action that, either directly or indirectly, results in unnecessary costs to the Medi-Cal / Medicaid programs.
- Any practice that does not provide Medi-Cal / Medicaid beneficiaries with services that are medically necessary, fairly priced, and meet professionally-recognized standards.
- Examples
  - Misusing codes on a claim
  - Charging excessively for services or supplies
  - Billing for services that were not medically necessary

TIPs for Safeguarding PHI

HIPAA requires that appropriate safeguards are in place to protect the privacy of Protected Health Information (PHI). Here are some tips on how you can do your part as a Holman Provider:

User Account Management

- ✓ User accounts on company computer systems are to be used only for business of the company and not to be used for personal activities.
- ✓ Users are personally responsible for protecting all confidential information created, used, transmitted, stored, and/or destroyed.
- ✓ Users are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons.
- ✓ User ID's should be unique. Workforce members are responsible for all actions associated with their user ID; therefore, it is important to ensure that a user ID is used only by the workforce member and no one else.
- ✓ Workforce members will be held responsible for the actions of another individual if he/she allows them to obtain and use their user ID and password or allow them access to patient information.

Network/ Workstation Rules

- ✓ Do not install unauthorized software onto a work PC or workstation.
- ✓ Do not attach any device that would alter the topology characteristics of the Network (e.g. USB thumb drives and writable CDs or DVDs).
- ✓ Position workstation monitors to be facing away from public view.
- ✓ Log off or lock computer workstation whenever leaving it unattended (Windows Button + L shortcut).
- ✓ Log off when leaving a workstation computer.
- ✓ Clean desk policy – do not leave materials containing PHI/ePHI on a workstation desk when leaving the workstation area.

Password Protection

Protecting passwords is a critical factor in protecting confidential information; therefore, passwords should be:

- ✓ Memorized and never written down in such a way that others can see or use them.
- ✓ Kept secret from others (do not share passwords).
- ✓ Be aware of scams to trick you into disclosing passwords through anonymous phone or email.
- ✓ Under no circumstances should anyone ever ask you for your password or should you voluntarily give it out.
- ✓ Collaborate with your network or system administrator to setup limited access to files or folders without having to share user IDs and passwords.
- ✓ Do not attempt to learn another person's password and/or access another person's account using their password.
- ✓ Strong passwords (alphanumeric, expiration, password history)
- ✓ Multi-factor authentication

Encourage staff member s to report any violations or suspected violations to their supervisor, a senior business leader, or Security officer within 24 hours.

TIPs for Safeguarding PHI (Cont.)

Faxes

- ✓ Avoid faxing confidential information. If you send a fax to an incorrect number, report the incident immediately to your Supervisor or Manager.
- ✓ Faxing sensitive PHI is strongly discouraged. Consider alternate method of transmission such as mail, SFTP, or email encryption.
- ✓ It is best practice to test a fax number prior to transmitting information. If this is not possible:
  - ✓ Restate the fax number to the individual providing it.
  - ✓ Obtain telephone number to contact the recipient with any questions.
- ✓ Do not include PHI on the cover sheet.
- ✓ Verify you are including the correct patient's information.
- ✓ The Fax Cover Sheet should contain a confidentiality notice requesting notification if the fax was delivered to the wrong person.

Emails

- ✓ Avoid opening any suspicious emails and attachments from unknown senders. Prior to opening/ reading emails review the email domain to ensure it was sent from a known person.
- ✓ Be aware of hypertext links within an email; it may be a scam.
- ✓ Keep e-mail content professional.
- ✓ Use work e-mail for work purposes only.
- ✓ Don't forward jokes.
- ✓ Emails that contain patient information that are sent outside of your organization must be encrypted.
- ✓ Verify the recipients email address before sending.
- ✓ Include a confidentiality disclaimer statement.

Note: Please contact The Holman Group (compliance@holmangroup.com) if you have questions regarding sending encrypted emails or need additional information on how to transmit encrypted information to The Holman Group.

Internet Activity

- ✓ Do not download any software or services.
- ✓ Do not answer yes to any prompts which offers a free update, or program that will speed up or increase your computer's performance, make your browser faster, etc.
- ✓ Do not click on any unfamiliar links within email or internet browser.
- ✓ Do not store company files, proprietary documents, or files containing PHI using web-based file sharing sites or services.

Consider implementing a Sanction Policy for improper/ unauthorized use of company property or behavior. Disciplinary actions may include coaching sessions, verbal warning, written warning, or termination of employment/ contractual obligations.

TIPs for Safeguarding PHI (Cont.)

Social Networking

- ✓ Social networking is now commonly used by businesses and with the general public and is a useful tool for certain business operations.
- ✓ While social networking can be useful, if improperly used, it can result in a variety of adverse consequences, such as disclosure of sensitive or PHI/PII information, copyright violations, and potential damage to your organization.
- ✓ Do not post work-related information to a personal (non-work related) social networking website.
- ✓ Do not use your work email address to use non-work web applications.

Family, Friends and Famous

- ✓ Do not share with family, friends, or anyone else a patient's name, or any other information that may identify him/her, for instance:
  - ✓ It would not be a good idea to tell your friend that a particular patient was seen after a severe drug overdose or mental breakdown.
- ✓ Do not inform anyone that you know a famous person, or their family members, were seen at your organization. This includes seeing data about a famous person.

Transporting Paper Records

If asked to transport paper records/PHI to another department:

- ✓ Secure so you don't drop them.
- ✓ Carry them close to your person.
- ✓ Carry them in a facility designated bag, box, or container.
- ✓ Ensure no names are visible.
- ✓ Ensure no records are left unattended.

If asked to transport paper records/PHI externally:

- ✓ Place in a locked briefcase, closed container, sealed, self-addressed interoffice envelope;
- ✓ Place PHI in the trunk of your vehicle, if available, or on the floor behind the front seat;
- ✓ Lock vehicles when PHI is left unattended.

Disposal of PHI

- Shred or place all confidential paper (including PHI) in the designated confidential paper bins
- For electronic media (floppy disk, CD, USB Drive, etc.), provide media to your organizations appropriate department for proper disposal.
- All computing equipment should be sanitized prior to hand over to a secure disposal facility

Business Continuity and Disaster Recovery

It is critically important for business organizations to be prepared for the worst with a solid but flexible Business Continuity Plan.

Business Continuity: The ability a company has to communicate with employees and continue operations in the face of a crisis, including: closure of the primary facility, loss of a key leader, severe natural disaster, failure of key hardware / systems, etc.

Disaster Recovery: The ability to restore network and computing resources to continue IT operations if they primary data center is compromised.

Do I need to comply with HIPAA rules?

Answer: The HIPPA Rules apply to covered entities and business associates. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules. Visit the HHS Cover Entity and Business Associates webpage for further details regarding "business associate" and "covered entity"; 45 CFR 160.103.

Covered Entities

A covered entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs.	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Business Associate

A business associate is defined as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

> *Note: A member of the covered entity's workforce is not a business associate; however a covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.*

Business Associates may include, but are not limited to;

- Third party claims processor
- CPA Firm who may have access to PHI information
- Legal attorney or counsel who may have access to PHI information
- Utilization review consultant
- Health care clearinghouse
- Translation servicer
- Accreditations

If a covered entity enters into an agreement for services with a business associate, a written contact or other arrangement must contain the elements specified at 45 CFR 164.504(e).

Enforcement

The HHS Office for Civil Rights enforces the HIPAA privacy, security, and breach notification rules. Violations of the rules may result in civil monetary penalties or, in some cases, criminal penalties enforced by the U.S. Department of Justice. Visit the HHS HIPAA Compliance and Enforcement webpage for more information.