Health Insurance Portability and Accountability Act (HIPAA) and PSH

The Health Information Portability and Accountability Act (HIPAA) is a federal law that (among other things) establishes national standards to protect sensitive patient information from being disclosed without the patient's knowledge or consent. As a Medicaid provider and a business associate of Amerigroup, the third-party administrator of the Foundational Community Supports program, Permanent Supportive Housing (PSH) providers are subject to HIPAA privacy and security standards and regulations.

HIPAA can be complicated, and its enforcement is rigorous and closely scrutinized. This is because personally identifiable health information is private, valuable, and sensitive. While many PSH providers have experience managing sensitive, confidential information, becoming a Business Associate to a Covered Entity means complying with expansive and evolving standards regarding how protected health information is generated, stored, and exchanged. This can represent a sharp learning curve.

HIPAA 101

HIPAA regulates how Protected Health Information (PHI) can be **used** and **disclosed** by **Covered Entities** and their **Business Associates**. It creates (and enforces) a national baseline privacy right and right of access for patients. Under HIPAA, Covered Entities and Business Associates have a duty of stewardship for PHI under their control. This means that in addition to restricting what can be done with PHI, **there is a positive duty to secure and protect PHI**.

Let's break that down with some definitions.

HIPAA is composed of four (4) primary components:

1. The Privacy Rule;
2. The Security Rule;
3. The Breach Notification Rule;
4. The Enforcement Rule.

The Department of Health and Human Services Office for Civil Rights (OCR) enforces HIPAA.

Who Does HIPAA Apply To?

HIPAA applies to Covered Entities (health insurers, health providers, and healthcare clearinghouses) and their Business Associates. Business Associates are persons or entities that contract with a covered entity to perform activities that involve the use or disclosure of PHI.

For a Covered Entity to properly share PHI with a Business Associate, there must be a Business Associate Agreement (BAA). This written agreement ensures that the Business Associate is held to the same standards of data stewardship as the covered entity, including the duty to notify the Covered Entity of any violations and data breaches.

What This Means For PSH Providers:

When contracting to become a PSH Provider, organizations will attest that they either are a Covered Entity (and are those qualified to receive PHI under the Treatment, Payment, and Operations HIPAA exception) or that the organization will enter into a valid BAA before the exchange of any PHI. Therefore, PSH providers that are not healthcare providers will need to review and execute a BAA as part of the contracting process. These BAAs mean that, by contract, PSH Providers will be held to the same standards as the Covered Entity (Amerigroup) regarding the protection, use, and disclosure of PHI.

PSH Providers must review the BAA closely to ensure they can implement and comply with all terms. This includes implementing processes to monitor, detect, and respond to potential violations and data security breaches.

What is "Protected Health Information"?

Protected Health Information (PHI) is any information about health status, healthcare delivery, or payment that is (1) created or collected by a Covered Entity or Business Associate that (2) can be linked back to a specific individual. This includes any part of a patient's medical record and payment history.

Put Simply: **PHI = (medical or health information) + (a personal identifier)**

OCR has published guidance identifying 18 types of personal data or identifiers[1] constituting PHI. Many of these are intuitive (e.g., names, identification numbers, biometric data), but it also includes IP address numbers and geographical identifiers smaller than the state level (some exceptions).

PHI applies any personally identifiable protected health information – regardless of the format of that data. This means that PHI can be written, recorded, or electronic. Electronic PHI is known as ePHI.

What This Means For PSH Providers:

PSH Providers need to be aware that just because THEY are not providing direct health services doesn't mean that the data they receive and generate isn't PHI. To be eligible for PSH services under Apple Health (Medicaid), an individual must have at least (1) one qualified health need; and (2) one defined risk factor.

The qualification for referral to PSH services is based on an individual's health and health needs assessment and constitutes PHI. This applies not only to information that PSH Providers receive from Covered Entities but to the information that PSH Providers generate themselves.

THE PRIVACY RULE (45 CFR § 160 and §164 Subparts A and E)

The Privacy Rule represents the core of HIPAA, and all other rules relate to the Privacy Rule in some way. The rule:

1. Requires appropriate controls or safeguards to protect the privacy of PHI. This includes limits on the conditions under which PHI may be used or disclosed.
2. Gives individuals rights over their PHI. This includes the right to examine and collect a timely copy of their health records, to direct the sharing ("transmittal") of their PHI to others, and to request corrections to the record.

In general, a Covered Entity or Business Associate can only **use** or **disclose**[2] PHI if either: (1) the Privacy Rule specifically permits or requires it; or (2) the individual who is the subject of the information gives authorization for its use or disclosure in writing.

The Minimum Necessary Requirement

The Privacy Rule permits the use and disclosure of PHI where necessary for treatment, payment, and healthcare operations. This is commonly known as the "TPO Exception." These are broadly construed and are considered routine disclosures. However, even when a Covered Entity or Business Associate is operating in the TPO exception, it is still responsible for making reasonable efforts only to access and use the minimum amount of PHI necessary to meet its goal (i.e., appropriate use).

This is known as the Minimum Necessary Requirement or "Minimum Use." It means that Covered Entities and Business Associates must make reasonable efforts to ensure that access to PHI is restricted to a particular purpose, use, disclosure, or request.

This Minimum Necessary Requirement plays out at both a practice or systemic level and on an individual level. This means that the Covered Entity or Business Associate is responsible for setting up default settings that restrict access to PHI to appropriate (minimum) use.

Examples of what this looks like in practice:

- A healthcare provider restricts which staff members have access to Electronic Health Records so that only those individuals who need to access PHI to perform their jobs have routine or direct access to records.
- A nurse providing care management services only has access to the medical records of those patients assigned to them.
- When sending a referral or sharing information with another provider on a patient, a healthcare provider only includes the personal identifiers and health information relevant to the interaction or purpose, redacting or not including multiple identifiers or extraneous health information.

Examples of what this looks for a PSH provider:

- Access to electronic documents and folders (including referral intake, case records and documentation, and billing) is segregated so that only staff with a legitimate and routine need based on job responsibilities can access individual folders containing this information.
- When sending information to other agencies and organizations related to a PSH client, a case worker limits the information provided to only include what is necessary and relevant to the communication. For example, in a communication with a landlord, the caseworker does not attach the entire case file or include multiple identifiers.

THE SECURITY RULE (45 CFR § 160 and §164 Subparts A and C)

Under the Privacy Rule, Covered Entities and Business Associates must safeguard and protect the confidentiality of all PHI. PHI applies any personally identifiable protected health information – regardless of the format of that data. This means that PHI can be written, recorded, or electronic. The Security Rule establishes *additional* standards and protections for **electronic PHI** (ePHI).

This includes the requirement to "implement policies and procedures to prevent, detect, contain, and correct security violations."[3] This is based on the recognition that the nature (and ubiquity) of electronic records present unique risks to the confidentiality, integrity, and security of those records.[4] The Security Rule creates a positive and iterative duty to identify, evaluate, and protect against the actions of third parties that present a cybersecurity risk to the confidentiality, integrity, and availability of patient information.

Covered Entities and their Business Associates, therefore, must use appropriate administrative, physical, and technical safeguards to:

1. Protect the confidentiality, accessibility, and integrity of all ePHI they create, maintain, receive, or transmit records;
2. Identify and protect against reasonably foreseeable threats to the security or integrality of ePHI in their stewardship;
3. Identify and protect against reasonably foreseeable uses or disclosures of ePHI, and
4. Institute controls to ensure compliance across their workforce.

These duties apply to ePHI "at rest" (or stored by the organization) and all data exchanges.

What Are Administrative Safeguards?

Administrative Safeguards are the policies and procedures an organization uses to select, develop, implement, and maintain the security measures deemed necessary to protect ePHI and manage the conduct of the organization's workforce as it relates to ePHI.

*All Covered Entities and Business Associates must perform a **periodic risk analysis** to:*

1. Identify potential risks to ePHI, including network vulnerabilities and threats,
2. Evaluate the likelihood and impact of those risks;
3. Identify and implement security controls to address the risks identified; and
4. Institute a process to continue to measure the adequacy and effectiveness of those security protections.

Other administrative safeguards or controls include:

- Policies and processes outlining the security management process and assigning accountability and responsibility for security controls;
- Workforce training on cybersecurity threats and data management;
- Business Continuity and contingency plans;
- Sanction or Disciplinary policies.

What are Physical Safeguards?

Physical safeguards refer to the steps taken to protect the physical security of the locations where ePHI may be stored, maintained, or accessed by a covered entity or business associate. Covered Entities and Business Associates must secure and control access to the facilities, workstations, and devices used to store, exchange, or access ePHI. Some examples of physical safeguards include:

- Alarm systems;
- Locking areas where ePHI is stored (server rooms, workstation areas);
- Maintaining a visitor log and identification and escort policy; and
- Placement of workstations to avoid accidental disclosures;

What are Technical Safeguards?

Technical safeguards include all the technical measures used to secure ePHI. Technical safeguards must consist of the following:

1. ***Access Controls:*** These are the technical policies and procedures to ensure that only authorized persons have access to ePHI. Examples include passwords, firewalls, encryption, penetration testing, etc.
2. ***Audit Controls:*** The mechanisms by which an organization can record and evaluate access to information systems containing ePHI.
3. ***Integrity Controls:*** The mechanisms by which an organization can monitor, detect, and prevent the unauthorized alteration or destruction of ePHI.
4. ***Transmission Controls:*** The measures by which an organization protects again unauthorized access (i.e., interception, misdirection, or malfeasance) of ePHI that is transferred electronically.

THE BREACH NOTIFICATION RULE (45 CFR §§ 164.400-414)

The Privacy Rule and the Security Rule outline the responsibilities Covered Entities, and their Business Associates have as it relates to protecting against impermissible use or disclosure of PHI. The Breach Notification Rule governs what happens when there is an impermissible use or disclosure of PHI that compromises the security or privacy of the information. Under this rule, Covered Entities and Business Associates have a duty to (1) promptly notify individuals affected by the Breach ("individual notice") and (2) notify the Secretary of HHS of all Breaches. In certain instances (when a breach impacts 500 or more individuals), prompt notice must be made to the Secretary of HHS **and** the media.

But let's start by defining what constitutes a Breach.

A breach occurs when there is unauthorized use or disclosure of PHI, and that unauthorized use results in an actual impact on the privacy or security of that information.

BREACH = (impermissible use or disclosure of PHI) + (actual impact on privacy or security)

It can be tough to assess impact immediately, so any unauthorized use or disclosure of unsecured PHI is presumed to be a breach unless the Covered Entity or Business Associate can demonstrate a low probability that the PHI's security or confidentiality has been compromised. To do this, the Covered Entity or Business Associate must complete a risk assessment that evaluates:

1. The nature and extent of the PHI involved (i.e., what types of identifiers are involved, the likelihood of re-identification, and the sensitivity of the information involved);
2. The identity of the unauthorized user or the individual to whom the PHI was disclosures, including the likelihood or risk of redisclosure;
3. Whether the PHI was actually received or viewed; and
4. The extent to which the risk has or can be mitigated.

THE ENFORCEMENT RULE (45 CFR §§ 160, Subparts C, D, and E)

The Enforcement Rule details the authority of OCR in investigating HIPAA violations and the availability of Civil Monetary Penalties and criminal penalties for intentional non-compliance with HIPAA.

Civil Monetary Penalties are intended to act as a deterrent, so the fines levied can be very significant, particularly as they are assessed individually (i.e., each PHI impacted constitutes an individual basis).

Penalties are assessed based on a four-tiered system based on the degree of perceived culpability (as determined by OCR), which ranges from where a violation occurred despite reasonable efforts to instances of neglect that go uncorrected for over 30 days. There is an annual limit (approximately $1.9 million) for any violation (but note that there are frequently multiple types of violations in any investigation).

Covered entities and individuals may be subject to criminal penalties, including imprisonment for intentional non-compliance with HIPAA protections.

ENDNOTES

[1] "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule," U.S. Department of Health and Human Services. October 25, 2022. Available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

[2] "Use" refers to the access, exchange, or utilization of PHI within an organization. "Disclosure" is the release, transfer or sharing access to PHI to anyone outside that organization.

[3] 45 C.F.R. § 164.308(a)(1).

[4] The Security Rule is built around protecting the confidentiality, integrity, and availability of ePHI. Confidentiality here means that ePHI is restricted to appropriate uses and disclosures, consistent with the Privacy Rule. Integrity means that the ePHI is not altered or destroyed in an unauthorized manner. Finally, "availability" means that the ePHI is accessible and usable "on demand" by an authorized person for an appropriate purpose..