HIPAA For Language Service Providers: A Primer

LUNA | Language Services

Overview

Many interpreters and translators perform work for hospitals and other entities in the healthcare industry. When performing this work, language service providers must comply with federal rules and regulations governing the privacy and security of patient healthcare information. This primer is designed to provide language service providers with a basic overview of these requirements, key terminology, and some practical tips and resources to help ensure compliance with the law.

This primer is intended only as a summary of certain provisions under the law; it should not be relied on as an comprehensive guide and further compliance efforts may be necessary.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes, among other things, a legal framework for the protection of medical patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of protected health information. There are two primary "Rules" with which language service providers should be familiar: (1) the "Privacy Rule" and (2) the "Security Rule."

The HIPAA "**Privacy Rule**" establishes national standards designed to protect individuals' medical records and other personal health information. The Rule requires appropriate safeguards to protect the privacy of this information and sets limits and conditions on how it is used and disclosed without patient authorization.

The HIPAA "**Security Rule**" establishes national standards designed to protect individuals' ***electronic*** personal health information that is created, received, used, or maintained by a covered entity (see definition below). The Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of this electronic information.

Who is Covered by HIPAA?

"Covered Entity"

Those who must comply with HIPAA are often called "**covered entities**." Whether an individual or organization, these entities include (1) health plans, (2) health care

clearinghouses, and (3) health care providers who electronically transmit health information in connection with transactions regulated by the Department of Health and Human Services.

Common examples of covered entities include hospitals, physician offices, pharmacies, and health insurance companies.

"Business Associate"

In general, a "**business associate**" is a person or organization not directly employed by a covered entity but instead performs certain functions or activities for or on behalf of a covered entity that involve the use or disclosure of individually identifiable health information. **Examples** of functions or activities include claims processing, data analysis, and billing, among other things.

An **interpreter or translator** becomes a business associate when providing their professional services to a covered entity, whether on-site or remotely. Any **subcontractors** working for the interpreter or translator are likewise considered business associates.

What Information is Protected?

The Privacy and Security Rules protect all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media (electronic, paper, or oral). The Privacy Rule calls this information "**protected health information**" or **PHI**.

Examples of PHI include medical records; biometric data; names and addresses (including email addresses); telephone/fax numbers; social security numbers; medical record numbers; dates of birth, death, admission, discharge; and full-face photos and comparable images of patients.

When Can PHI be Used or Disclosed?

You may use or disclose PHI **only to the extent necessary to perform the services for which you've been hired**. In other words, only those who need to access PHI to do their jobs should get to see it. And unless a person has a specific need for PHI, access must be restricted. The U.S. Department of Health and Human Services refers to this as the "**minimum necessary standard**."

While impossible to determine every circumstance in which this standard applies, always ask yourself, before using or sharing PHI, "Is this necessary, or can the job be done without this

information?" If you're unsure, always air on the side of caution and refrain from use or disclosure.

Examples of when it may be appropriate to use or disclose PHI include:

- The facilitation of communication between the patient and physician or the physician and others contributing to the patient's care;
- Receiving payment for services provided to a patient; and
- Other legitimate business purposes

Some Practical Tips on How to Protect PHI

Here are some practical tips on how to keep PHI protected:

- **Never share sensitive PHI** with others who shouldn't have access, including co-workers or personal acquaintances.
- If you are required to share PHI, **share the minimum amount of information necessary** to accomplish the task at hand.
- **Secure all paperwork** containing PHI by placing in a drawer or folder when not in use; never leave records and other PHI unattended.
- **Limit e-mail transmissions of PHI** to only those circumstances when the information cannot be sent another way.
- **Password protect all devices** and computers that can access PHI. Never share your passwords.
- **Use adequate security** to send and receive information over **public Wi-Fi networks**.

Resources

American Medical Association, *HIPAA Privacy and Security Rules*, https://www.ama-assn.org/practice-management/hipaa-privacy-security-resources.

HealthIT.gov, *Guide to Privacy and Security of Electronic Health Information*, https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information.

U.S. Department of Health and Human Services, *Training Materials*, https://www.hhs.gov/hipaa/for-professionals/training/index.html.

Image Credit: *Medical Background Design*, by PhotoRoyalty via Freepik.com.

Last Updated: March 30, 2017.