Telehealth HIV Privacy and Security

Shefali Mookencherry, MPH, MSMIS, RHIA, CHPS, HCISSP

November 2020

Disclaimer: The materials for this paper are for informational purposes only. Information within this paper does not constitute legal or business advice. Information in this presentation is provided without warranty of any kind, either expressed or implied, including but not limited to, the implied warrantees of fitness for a particular purpose.

Contents

Executive Summary

Public health authorities (PHAs) must adhere to the confidentiality of HIV Protected Health Information (PHI). Many states as well as the federal government have laws that govern the use of, and serve to protect, identifiable information collected by public health authorities.

Services provided by PHAs may include the acquisition, use, and exchange of HIV PHI to perform public health activities (e.g.: public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research). This information may allow public health authorities to implement mandated activities (e.g., identifying, monitoring, and responding to birth, death, disease, and disability among populations) and complete public health objectives.

While it is important to conduct these services, public health authorities at times will need to comply with several federal and/or state regulations regarding the uses and disclosures of HIV PHI.

Specifically, this paper explores the Health Insurance Portability and Accountability Act (HIPAA) impacts on public health authorities' activities and telehealth HIV services provided. HIPAA established a base for rules and regulations to protect the privacy and security of HIV patient's health information—regardless of the PHI medium (verbal, written, and/or electronic).

Overview

Protection of a HIV individual's privacy has been a tradition among health care providers and public health practitioners in the United States. Previous legal protections at the federal, tribal, state, and local levels were inconsistent in policy, implementation, and enforcement. A spider web of laws attempted to provide narrow privacy protections for selected health data and certain maintainers of that data.

The U.S. Department of Health and Human Services (DHHS) addressed these concerns with new privacy and security standards that set a national minimum of basic protections, while balancing individual needs with those of society.

HIPAA as a Federal Law

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA required the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information and required the Department of Health and Human Services (DHHS) to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

The Act has five separate Titles. Title II of HIPAA, known as the Administrative Simplification provisions, required the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administrative Simplification provisions also addressed the security and privacy of health data. The standards were meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange.

The Administrative Simplification provisions standardized the exchange of electronic health information (administrative and financial), such as:

- Health plan enrollment (or disenrollment)
- Health plan eligibility determinations
- Health plan premium payments
- Referral certification, authorization
- Claim submissions (encounter info)
- Health plan benefit coordination
- Claim status inquiries

- Payment and remittance advices

Administrative requirements were established:

- Designate a privacy officer with primary responsibility for ensuring compliance with the regulations
- Establish training programs for all members of the workforce
- Implement appropriate policies & procedures to prevent intentional and accidental disclosures of PHI
- Establish a system for receiving and responding to complaints regarding the Covered Entity's privacy practices
- Implement appropriate sanctions for violations of the privacy guidelines
- Make reasonable efforts to limit information to minimum necessary to accomplish a person's purpose/job

Omnibus Rule

On January 25, 2013, the Department of Health and Human Services (HHS) published the "HIPAA Omnibus Rule," a set of final regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement various provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Compliance date was September 23, 2013; the Omnibus final rule provided the following:

1. The final rule expanded patient rights by allowing them to ask for a copy of their electronic medical record in electronic form.

2. Under the final rule, when patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan.

3. If a Medicare beneficiary requests a restriction on the disclosure of PHI to Medicare for a covered service and pays out of pocket for the service, the provider must also restrict the disclosure of PHI regarding the service to Medicare.

4. The final rule sets new limits on how information can be used and disclosed for marketing and fundraising purposes, and it prohibits the sale of an individuals' health information without their permission.

5. Penalties for noncompliance with the final rule were based on the level of negligence with a maximum penalty of $1.5 million per violation.

6. The breach notification final rule was amended with a requirement to determine the breach's "risk of compromise" rather than harm. "Compromise" was considered a more objective test than harm. Thus, breach notification is necessary in all situations except those in which the covered entity or business associate demonstrates a low probability that the PHI has been compromised.

7. To determine whether there is a low probability that PHI has been compromised; the covered entity or business associate must conduct a risk assessment that considers at least each of the following factors:

- 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.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

8. The final rule changed what incidents are exceptions to the definition of "breach." Before, an incident was an exception to the definition of breach if the PHI used or disclosed a limited data set that did not contain any birthdates or ZIP codes. Under the final rule, breaches of limited data sets — regardless of their content — must be handled like all other breaches of PHI.

9. Providers and covered entities still have a safe harbor, in which an unauthorized disclosure only rises to the level of a breach — thereby triggering notification requirements of the HITECH Act — if the PHI disclosed is "unsecured."

10. Unsecured PHI is PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technology or methodology specified by the secretary through published guidance.

11. Requirements for methods of breach notification remain unchanged. That is, providers and covered entities most provide notice to individuals, the media (if breach affects more than 500 residents of a state or smaller jurisdiction) and HHS (if breach affects more than 500 individuals regardless of location). Business associates, or people or organizations that conduct business with the covered entity that involves the use or disclosure of individually identifiable health information, must also provide notice to covered entities no later than 60 days after the discovery of a breach of unsecured PHI. (Read more about breach notification rules.)

12. Covered entities' Notice of Privacy Practices (NPPs) forms need to inform patients that they will be notified if their PHI is subject to a breach. NPPs must also inform individuals that a covered entity may contact them to raise funds, and the individual has a right to opt out of receiving such communications.

13. Business associate agreements and policies and procedures must address the prohibition on the sale of patients' PHI without permission.

14. Covered entities must modify and implement policies and procedures that address the new limits on permissible uses of information for marketing and fundraising activities.

15. Covered entities' business associate agreements and policies and procedures must address the expanded rights of individuals to restrict disclosures of PHI.

Lastly, under the Omnibus Rule, subcontractors (or agents) that perform services for a business associate are also considered business associates to the extent their services require access to PHI. A business associate is obligated to obtain satisfactory assurances from its HIPAA-covered subcontractors, in the form of a written agreement, that the subcontractor will appropriately safeguard the PHI. Entities that receive PHI only to assist a business associate with its own management and administration or legal responsibilities are not subcontractors (and, thus, not business associates). However, a business associate would be required to obtain reasonable assurances from such entities that the information would be held confidentially and only used or disclosed as required by law or for the purposes for which it was disclosed.

Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their 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 their third party service providers, pursuant to section 13407 of the HITECH Act.

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated

Unsecured PHI is defined as PHI that is not secured by technology or methodology that renders the PHI unreadable, unusable or indecipherable to unauthorized individuals. The HITECH Act provides only two methods for securing PHI: encryption and destruction. To be secure, PHI must either be encrypted under specific standards adopted by the National Institute of

Standards and Technology or must be destroyed so that it cannot be read or reconstructed.

Electronic PHI must be secured through encryption. Where PHI is encrypted, the encryption key must be kept on a separate device from the data being encrypted or decrypted to avoid a breach. PHI that is maintained in the form of paper, film or other hard copy media must be destroyed or shredded. Although other means of safeguarding PHI, such as access controls, firewalls or redaction, are acceptable under the Security Rule, unauthorized disclosure of data secured by these means may be considered breaches of unsecured PHI.

If unsecured PHI has been breached, the covered entity must notify the affected individuals without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The breach will be considered discovered on the first day it is known (or reasonably should have been known) to any member of the covered entity's workforce or an agent of the covered entity (other than the person who committed the breach).

If the breach involves more than 500 individuals in a single state or jurisdiction, the HITECH Act requires a covered entity to notify "prominent media outlets" in the relevant state or jurisdiction, which notice may be in the form of a press release.

A covered entity is required to report all breaches of unsecured PHI to HHS. If the breach involves 500 or more individuals, the covered entity is required to report the breach to HHS at the same time affected individuals are notified. See table below:

Providing Notification To…	**Breach Involved < 500 Individuals**	**Breach Involved ≥ 500 Individuals**
Individuals	No later than 60 days from discovery	No later than 60 days from discovery
HHS	Submit a log of all breaches once a year, no later than 60 days after end of calendar year	At same time as notice to individuals, no later than 60 days from discovery
Media	N/A	No later than 60 days from discovery

If a business associate is responsible for a breach of unsecured PHI, the business associate must notify the covered entity and provide the information necessary to permit the covered entity to provide the required notice. Notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. A breach is treated as

discovered by a business associate as of the first day on which such breach is known (or reasonably should have been known) to the business associate or to any person (other than the person committing the breach) who is an employee, officer, or other agent of the business associate.

HIPAA Privacy Rule

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

The Privacy Rule regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information, called protected health information (PHI). PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral), but excludes certain educational records and employment records. The three types of covered entities are: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.

In general, the Privacy Rule can be summarized as follows:

> "Covered entities" may not use or disclose "protected health information" (PHI) except as authorized by the individual who is the subject of the information, or as explicitly required or permitted by the regulation.

Even when the use or disclosure of PHI is permitted, in most circumstances, only the "minimum necessary" amount of information to accomplish the intended purpose of the use, disclosure or request may be provided. The rules apply to all protected health information maintained, used or disclosed by a covered entity, regardless of the form it takes – electronic, written or oral. This information remains protected during the life of the individual, and information about a deceased individual must remain protected as long as the covered entity maintains the information.

Among other provisions, the Privacy Rule:

- gives patients more control over their health information;
- sets boundaries on the use and release of health records;
- establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;
- holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights;

- strikes a balance when public health responsibilities support disclosure of certain forms of data;
- enables patients to make informed choices based on how individual health information may be used;
- enables patients to find out how their information may be used and what disclosures of their information have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

HIPAA Security Rule

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

Classification of State Public Health Departments

Public Health PHI

Public Health protected health information (PHI) includes the following:

- Immunizations registries/results
- Mental Health records
- Drug and Alcohol Abuse records
- AIDS/HIV test results
- Controlled substance medication history from IL prescription monitoring program (PMP)
- Newborn screenings (metabolic and hearing)
- Lead results
- STD results/registries
- Test results from state labs
- Communicable disease test results/registries (Tuberculosis)
- Cancer registries

- Other PHI held

Public Health Departments Performing HIV Covered Functions

Public health authorities at the federal, tribal, state, or local levels that perform covered functions (e.g., providing health care or insuring individuals for health-care costs), may be subject to the Privacy Rule's provisions as covered entities.

A public health authority that conducts health care as part of its activities is a covered health-care provider if it also performs electronic transactions covered by the HIPAA Transactions Rule as part of these activities.

Under the Privacy Rule, a health plan is an individual or group plan that provides, or pays the cost of, medical care. This specifically includes government health plans (e.g., Medicare, Medicaid, or Veterans Health Administration).

A public health authority might be a health-care clearinghouse if it receives HIV health information from another entity and translates that information from a nonstandard format into a standard transaction or standard data elements (or vice versa). Operators of community health information systems should carefully consider whether they meet the definition for a health-care clearinghouse.

A public health department/authority that is a covered entity, and has both covered and non-covered functions may become a hybrid entity by designating its health-care components. By designating itself as a hybrid entity, a public health authority can carve out its non-covered functions, so that the majority of Privacy Rule provisions apply only to its health-care component.

Understanding Business Associate and Trading Partner Relationships

Business Associates are an individual or organization that performs, or assists in the performance of, a function or activity on behalf of the covered entity, involving the use or disclosure of HIV PHI.

- Example – A billing service who processes claims for a provider is a business associate

Trading partners are an organization with whom a covered entity exchanges information electronically using a named transaction standard.

- Example - A provider and a clearinghouse can be trading partners

Telehealth HIV Privacy and Security

HIV Telehealth Defined

It is the use of HIV electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration. Technologies include videoconferencing, the internet, store- and-forward imaging, streaming media, and landline and wireless communications. Telehealth services may be provided, for example, through audio, text messaging, or video communication technology, including videoconferencing software. Telehealth has four modalities: live video, store-and-forward, remote patient monitoring, and mobile health. Live video refers to real-time, two-way interaction between a health care provider and a patient, caregiver, or other provider using audiovisual methods. Store-and-forward telehealth refers to recorded data transmission to a health care provider.

This HIV data includes videos or imaging like x-rays that may be sent via secure email. The practitioner will then use the data to provide a service or evaluate a health case outside of a live interaction. Remote patient monitoring (rPM) is when the health history from a patient at one location is transmitted to a provider at another location to use in the patient's care. Once a patient is home or placed in a care facility after an emergency room visit, for example, rPM allows providers to continue to track their medical data. Mobile health or mhealth refers to the use of technology like tablets and cell phones to support public health education and practice.

Uses and Disclosures of HIV PHI for Public Health

A public health authority is broadly defined as including agencies or authorities of the United States, states, territories, political subdivisions of states or territories, American Indian tribes, or an individual or entity acting under a grant of authority from such agencies and responsible for public health matters as part of an official mandate. Public health authorities include federal public health agencies (e.g., CDC, National Institutes of Health [NIH], Health Resources and Services Administration [HRSA], Substance Abuse and Mental Health Services Administration [SAMHSA], Food and Drug Administration [FDA], or Occupational Safety and Health Administration [OSHA]); tribal health agencies; state public health agencies (e.g., public health departments or divisions, state cancer registries, and vital statistics departments); local public health agencies; and anyone performing public health functions under a grant of authority from a public health agency [45 CFR § 164.501].

The Privacy Rule allows covered entities to disclose HIV PHI to public health authorities when required by federal, tribal, state, or local laws [45 CFR 164.512(a)]. This includes state laws (or state procedures established under such law) that provide for receiving reporting of disease or injury, child abuse, birth, or death, or conducting HIV public health surveillance, investigation, or intervention.

For disclosures not required by law, covered entities may still disclose, without authorization, to a public health authority authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, the minimum necessary information to accomplish the intended public health purpose of the disclosure [45 CFR 164.512 (b)].

For instance, these disclosures may be made:

(1) to the extent that the disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of that law;
(2) for certain public health activities. These might include disclosure to:

- a public health authority authorized by law to collect information to prevent or control disease or conduct public health surveillance;
- a public health authority empowered by law to receive reports of child abuse or neglect;
- under certain circumstances, to a person subject to the jurisdiction of the Food and Drug Administration (FDA);
- a person exposed to a communicable disease; or
- in certain circumstances, an employer regarding workplace-related medical surveillance activities.

(3) to a government authority authorized by law when the covered entity reasonably believes that an individual is a victim or abuse, neglect or domestic violence;
(4) for health oversight activities authorized by law, including, for instance, fraud and abuse audits, investigations, and civil, administrative, or criminal proceedings (except if the investigation or other activities does not arise out of and is not directly related to the receipt of health care or qualification or receipt of public health benefits or services);
(5) for judicial and administrative proceedings under certain circumstances;
(6) for law enforcement purposes to a law enforcement official. However, under this exception, only limited information may be disclosed for identification and location purposes, such as information about an individual who is a victim of a crime when the victim has agreed to the disclosure or when reporting a crime in an emergency;
(7) to organ procurement organizations regarding cadaver organs, eyes, or tissue for donation purposes;
(8) for research purposes provided that an Institutional Review Board (IRB) or privacy board (as described in §164.512(i)(B) of the regulation) approves the waiver of individual authorization required under §164.508 of the regulation and certain other conditions are met;
(9) to avert a serious threat to health or safety;
(10) for specialized government functions, such as separation or discharge from the military, to determine eligibility for veterans' health benefits, or for protective services for the President and others;

(11) to the extent necessary to comply with workers' compensation or other similar laws. Note that the exception permitting disclosure applies only when providing the information is required under these laws, not when the laws simply permit disclosure.

Furthermore, the Privacy Rule allows covered entities to use or disclose PHI without consent or authorization if the covered entity reasonably believes the patient is a victim of abuse, neglect, or domestic violence. The rule covers child abuse and other victims of abuse, neglect or domestic violence (e.g., abuse of nursing home residents or residents of facilities for the mentally retarded).

Covered entities can make such disclosures only to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence. The disclosure can be made only if:

- the disclosure is required by law and complies with and is limited to the relevant requirements of such law; or
- if the individual agrees to the disclosure; or
- to the extent the disclosure is expressly authorized by statute or regulation and
    1. the covered entity, in its professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
    2. if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI sought is not intended for use against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Once the covered entity discloses the HIV PHI, it must promptly inform the individual that a report has been made, unless:

- the covered entity, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm; or
- the covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing the representative would not be in the best interests of the individual.

In addition, the privacy rule treats psychotherapy notes as a distinct category of PHI. A covered entity must obtain the patient's consent (but not authorization) for the person who created the psychotherapy notes to use the notes to carry out treatment and for the covered entity to use

or disclose psychotherapy notes for conducting training programs in which students, trainees, or practitioners in mental health learn under supervision to improve their skills in counseling.

Also, the confidentiality of alcohol and drug abuse patient records is regulated under 42 C.F.R. Part 2. 42 C.F.R. Part 2 prohibits the disclosure and use of drug and alcohol abuse records maintained in connection with the performance of any federally assisted substance abuse program unless certain conditions exist. The Privacy Rule permits disclosures without patient consent for public health activities and directory assistance. These disclosures would not be permissible under 42 C.F.R. Part 2.

Emergency Declaration for Waiver of Privacy Rule Provisions

The Secretary of HHS may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

If the President declares an emergency or disaster *and* the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered entity that does not comply with certain provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 CFR 164.510(b))
- the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a))
- the requirement to distribute a notice of privacy practices (45 CFR 164.520)
- the patient's right to request privacy restrictions (45 CFR 164.522(a))
- the patient's right to request confidential communications (45 CFR 164.522(b))

Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations.

- For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient's location. See 45 CFR 164.510(b)(4).

In March 2020, the Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency was issued by the Office of Civil Rights (OCR). During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote

communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

A covered health care provider that wants to use audio or video communication technology to provide telehealth to HIV patients during the COVID-19 nationwide public health emergency:

- Can use any **non-public facing** remote communication product that is available to communicate with patients.
- May provide similar telehealth services in the exercise of their professional judgment to assess or treat any other medical condition, even if not related to COVID-19, such as a HIV or other conditions.
- May use applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency.
- Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are **public facing**, and should not be used in the provision of telehealth by covered health care providers. Vendors listed below may provide HIPAA-compliant video communication products and may enter into a HIPAA BAA:

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams

- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger

Public Health Departments should enter into a HIPAA BAA with telehealth or video-conferencing vendors. Some examples of what OCR may consider a bad faith provision of telehealth services include:

- Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
- Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (e.g., sale of the data, or use of the data for marketing without authorization);
- Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (i.e., based on documented findings of a health care licensing or professional ethics board); or
- Use of public-facing remote communication products, such as TikTok, Facebook Live, Twitch, or a public chat room, which OCR has identified in the Notification as unacceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication.

Telehealth HIV Informed Consent

The TCPA (Telephone Consumer Protection Act) is a federal statute enacted in 1991 designed to safeguard consumer privacy including HIV patients. This legislation restricts telemarketing communications via voice calls, SMS texts, and fax. The Telephone Consumer Protection Act requires:

- to obtain prior express written consent from consumers before robocalling them.
- to no longer allow telemarketers to use an "established business relationship" to avoid getting consent from consumers when calling home phones, and
- to require telemarketers to provide an automated, interactive "opt-out" mechanism during each robocall so consumers can immediately tell the telemarketer to stop calling.

Public health departments must obtain informed consent from HIV client/patient in order to use telehealth for healthcare services.

PrEP Telehealth

Regarding pre-exposure prophylaxis (PrEP), telehealth specifically refers to the delivery of PrEP related clinical services to prevent HIV. Where PrEP telehealth is available, those receiving PrEP can now have virtual visits with their provider, as opposed to having a physical visit.

- May increase PrEP access for those most vulnerable to HIV who may not otherwise have access due to social stigma or distance from the closest PrEP provider.
- May reduce PrEP delivery barriers related to local health care professional shortages since, again, patients do not necessarily have to physically visit a provider.
- May support patients who struggle with medication adherence.

The development and use of real-time electronic adherence monitors, digital medicine systems, and short message service (SMS) surveys in PrEP research illustrates technology advances that may improve adherence measurements. PrEP services provided via a telehealth platform may include:

- HIV patients can have a virtual visit with their physician or care team.
- Physician can order PrEP-related tests at a local lab.
- A 90-day prescription for PrEP medication can be sent to the patient's preferred pharmacy once the labs are reviewed.
- Provider can send reminders when patients need to have repeat lab testing or have another visit with their physician to continue receiving PrEP prescriptions.

Accounting for HIV PHI

The Privacy Rule allows disclosures of PHI to public health authorities. Covered entities must comply with certain requirements related to these disclosures. One such requirement is that a covered entity must be able to provide an individual, upon request, with an accounting of certain disclosures of HIV PHI. The required accounting for disclosures may be accomplished in different ways. Typically, the covered entity must provide the individual with an accounting of each disclosure by date, the HIV PHI disclosed, the identity of the recipient of the HIV PHI, and the purpose of the disclosure. However, where the covered entity has, during the accounting period, made multiple disclosures to the same recipient for the same purpose, the Privacy Rule provides for a simplified means of accounting.

The date of each disclosure need not be tracked. Rather, the accounting may include the date of the first and last such disclosure during the accounting period, and a description of the frequency or periodicity of such disclosures. For example, the different amount of data exchanged between covered entities and public health authorities is made through ongoing, regular reporting or inspection requirements. A covered health-care provider may routinely report all cases of measles it diagnoses to the local public health authority. An accounting of such disclosures to a requesting individual would need to identify the public health authority receiving the PHI, the PHI disclosed, the purpose of the disclosure (e.g.: required for communicable disease surveillance), the periodicity (weekly), and the first and last dates of such disclosures during the accounting period (May 1, 2015 to June 1, 2015).

Notice of Privacy Practices for HIV PHI

Under the Privacy Rule, individuals have the right to adequate notice of the uses and disclosures of HIV PHI that may be made by the covered entity, as well as their rights and the covered entity's legal obligations.

Minimum Necessary for HIV PHI

Even if the covered entity is authorized to use or disclose HIV PHI, it must make reasonable efforts to limit HIV PHI to the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

As an operational matter, the "minimum necessary" determination should begin with an assessment of whether or not the intended use or purpose could be accomplished by de-identifying the data or using summary data, rather than assuming that all protected health information may be disclosed, and then attempting to narrowing the scope of disclosure of PHI to comply with the minimum necessary rule.

HIPAA's Effect on Public Health Reporting

A public health reporting requirement may be specifically authorized via legislation or administrative regulation, which may obligate the public health department to perform the activity to protect the public's health.

The Privacy Rule recognizes the important role that persons or entities other than public health authorities play in certain essential public health activities. Accordingly, the Rule permits covered entities to disclose protected health information, without authorization, to such persons or entities for the public health activities discussed below.

- Child abuse or neglect. Covered entities may disclose protected health information to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive

such reports. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization. Likewise, a covered entity could report such cases to the police department when the police department is authorized by law to receive such reports. See 45 CFR 164.512(b)(1)(ii). See also 45 CFR 512(c) for information regarding disclosures about adult victims of abuse, neglect, or domestic violence.

- Quality, safety or effectiveness of a product or activity regulated by the FDA. Covered entities may disclose protected health information to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples of purposes or activities for which such disclosures may be made include, but are not limited to:
    - Collecting or reporting adverse events (including similar reports regarding food and dietary supplements), product defects or problems (including problems regarding use or labeling), or biological product deviations;
    - Tracking FDA-regulated products;
    - Enabling product recalls, repairs, replacement or look back (which includes locating and notifying individuals who received recalled or withdrawn products or products that are the subject of look back); and
    - Conducting post-marketing surveillance.

  See 45 CFR 164.512(b)(1)(iii). The "person" subject to the jurisdiction of the FDA does not have to be a specific individual. Rather, it can be an individual or an entity, such as a partnership, corporation, or association. Covered entities may identify the party or parties responsible for an FDA-regulated product from the product label, from written material that accompanies the product (known as labeling), or from sources of labeling, such as the Physician's Desk Reference.

- Persons at risk of contracting or spreading a disease. A covered entity may disclose protected health information to a person who is at risk of contracting or spreading a disease or condition if other law authorizes the covered entity to notify such individuals as necessary to carry out public health interventions or investigations. For example, a covered health care provider may disclose protected health information as needed to notify a person that (s)he has been exposed to a communicable disease if the covered entity is legally authorized to do so to prevent or control the spread of the disease. See 45 CFR 164.512(b)(1)(iv).
- Workplace medical surveillance. A covered health care provider who provides a health care service to an individual at the request of the individual's employer, or provides the service in the capacity of a member of the employer's workforce, may disclose the individual's protected health information to the employer for the purposes of workplace medical surveillance or the evaluation of work-related illness and injuries to the extent the employer needs that information to comply with OSHA, the Mine Safety and Health Administration

(MSHA), or the requirements of State laws having a similar purpose. The information disclosed must be limited to the provider's findings regarding such medical surveillance or work-related illness or injury. The covered health care provider must provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the worksite if that is where the service is provided). See 45 CFR 164.512(b)(1)(v).

Information Blocking Act and HIV

Published on May 1, 2020, the 21st Cures Act Information Blocking Regulations ("Regulations") have a compliance date of November 2, 2020. These Regulations reflect a paradigm shift in how health care providers must provide access to electronic health information. Further guidance is pending from CMS and OIG regarding enforcement of the rule; however, exclusion and $1 million per violation civil monetary penalties are all still possible. The Regulations are not simply a technical responsibility that rests solely with the CIO, but rather compliance with these obligations requires participation by clinical staff, IT, privacy, security and legal to identify practices and activities that appear to discourage the access, exchange or use of EHI and to develop a process to (a) receive requests for access; (b) evaluate those requests in the context of some very specific exceptions; and (c) respond to requests within a defined period of time (depending on the applicability of the exception the time period can be as short as 10 days).

These Regulations impart risk on many activities that have come to be common practice (e.g., standing order to holding HIV test results until counseling services are coordinated, production of limited data in response to records request, etc.). These Regulations are requiring health systems to re-evaluate how they maintain and make available patient information.

HIPAA Compliance

HIPAA Compliance Assessment

HIPAA compliance activities could involve the following:

- Review and modification of privacy and security policies and procedures
- Designation of Privacy Officer with authority
- Develop a HIPAA Training Program
- Establish a HIPAA Complaint Process
- Establish an internal compliance audit program
- Enforce sanctions as necessary
- Develop and implement incident response and corrective action procedures
- Perform PHI/ePHI inventory
- Update Notice of Privacy Practices
- Review and identify all Business Associates
- Update Business Associate Agreements
- Update breach notification policies and procedures

- Develop and train employees on new policies (patient requested PHI restrictions, patient requested electronic copies of PHI, breach notification, etc)
- Review and update authorization and other forms as necessary

A HIPAA Compliance assessment should be performed at least yearly.

HIPAA IT Security Risk Analysis

The Security Management Process standard in the Security Rule requires organizations to"[i]mplement policies and procedures to prevent, detect, contain, and correct security violations." (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

> RISK ANALYSIS (Required).
> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

In addition to an express requirement to conduct a risk analysis, the Rule indicates that the risk analysis is a necessary tool in reaching substantial compliance with many other standards and implementation specifications. For example, the Rule contains several implementation specifications that are labeled "addressable" rather than "required." (68 FR 8334, 8336 (Feb. 20, 2003).) An addressable implementation specification is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so. (See 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306(d)(3).)

A HIPAA security risk analysis should be performed at least yearly. In summary, Risk analysis is the first step in an organization's Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.

HIPAA Training/Education

The HIPAA privacy and security rules require formal education and training of the workforce to ensure ongoing accountability for privacy and security of protected health information (PHI). HIPAA's privacy and security rules independently address training requirements.[1] Like most standards, the training requirements are non-prescriptive, giving organizations flexibility in implementation.

Note the below excerpts from the Privacy and Security Rules regarding training:

HIPAA Privacy Rule

Section 164.530 of the HIPAA privacy rule states:

(b) 1. **Standard: training.** A covered entity must train all members of its work force on the policies and procedures with respect to PHI required by this subpart, as necessary and appropriate for the members of the work force to carry out their function within the covered entity.

(b) 2. **Implementation specifications: training.**

i. A covered entity must provide training that meets the requirements of paragraph (b) (1) of this section, as follows:

- To each member of the covered entity's work force by no later than the compliance date for the covered entity
- Thereafter, to each new member of the work force within a reasonable period of time after the person joins the covered entity's work force
- To each member of the covered entity's work force whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section

ii. A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

HIPAA Security Rule

HIPAA's security standard 164.308(a)(5)(i) states:

...Implement a security awareness and training program for all members of its work force (including management).

(ii) Implementation specifications. Implement:

- Security reminders
- Protection from malicious software
- Log in monitoring
- Password management

A covered entity must train the entire workforce on HIPAA-directed privacy policies and procedures necessary to comply with the rule. Workforce training should be executed through normal or existing organizational educational operations. All covered entities must provide

ongoing updates and document evidence of compliance in written or electronic form and retain it for a minimum of six years from the implementation date.

Covered entities should train the entire workforce, including management, on security issues respective of organizational uniqueness. In addition, the covered entity periodically should provide security training updates based on technology and security risks.

Appendices

Definitions

Business Associate Definition

The HIPAA definition of Business Associate has broad applicability and includes, other than a health care provider's employees, "partners" that may provide legal, actuarial, accounting, consulting, data aggregation, management, administration or financial services wherein the services require the *disclosure of individually identifiable health information.*

Clearinghouse

“Health care clearinghouses” are public or private entities (including billing companies or community health management information systems) that either (1) process or facilitate processing of health information received from another entity in a nonstandard format into standard data elements or a standard transaction; or (2) receive a standard transaction from another entity and process or facilitate processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

Covered Entity Definition

The HIPAA definition of covered entity means:

1. A health plan,
2. A health care clearinghouse, or
3. A health care provider who ***transmits*** **any health information in electronic form in connection with a transaction covered by this subchapter.**

Disclosure

The HIPAA definition of disclosure means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information.

Electronic Media

The HIPAA definition of electronic media is broadly defined and includes both (1) electronic storage and (2) electronic transmission media. That said, the following language within this definition excludes certain transmission:

Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Health Care

The HIPAA definition of Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Operations

"Health care operations" includes certain services or activities necessary to carry out the covered functions of the covered entity with respect to treatment or payment, such as conducting quality assessment and improvement activities, outcomes evaluation and development of clinical guidelines (providing that obtaining generalizable knowledge is not the primary purpose of any studies resulting from these activities), population-based activities related to improving health or reducing health care costs, coordinating or managing care, evaluating provider performance, engaging in accreditation, certification or licensing activities, underwriting or premium rating for purposes of creation, renewal, or replacement of a contract of health insurance or health benefits, conducting or arranging for medical review, legal services, and auditing (including detection of fraud and abuse), business planning or development, management activities, customer service, resolution of internal plan grievances, and due diligence in connection with the sale or transfer of assets to a potential successor in interest.

Health Care Provider

The HIPAA definition of health care provider means, in general, services performed by physicians, and services performed by a host of other health care professionals, as defined in 42 U.S.C. 1395x(s) and 1395x(u), and any other person or organization "who furnishes, bills, or is paid for health care in the normal course of business."

Individually Identifiable Health Information

The HIPAA definition of Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

i. That identifies the individual; or
ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Payment

"Payment" includes activities undertaken by a health plan or provider to obtain or provide reimbursement or premiums for the provision of health care and other activities, such as determinations of eligibility or coverage (including coordination of benefits), risk adjustments, billing, claims management, collections, medical necessity reviews, and utilization review.

Protected Health Information (PHI)

The HIPAA definition of protected health information means individually identifiable health information:

1. Transmitted by electronic media; or
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium.

Treatment

"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers. It also includes coordination or management of health care by a health provider and a third-party and consultation or referrals between one health care provider and another.

Use

The HIPAA definition of Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce

The HIPAA definition of Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

References

[42 C.F.R. §2.12 (a)(i)-(ii)].
[42 C.F.R. §2.12 (b)].
[42 C.F.R. §2.12 (e)(1)].
[42 C.F.R. §2.11].
[45 CFR § 160.103].
[45 CFR 160.306].
[45 CFR 160.312].
[45 CFR § 164.501].
[45 CFR § 164.502 (a)].
[45 CFR § 164.504(e)(1)].
[45 CFR § 164.504(e)(3)].
[45 CFR § 164.506, 65 Fed. Reg. 82810].
[45 CFR § 164.508, 65 Fed. Reg. 82811].
[45 CFR § 164.508(a)(2)].
[45 CFR § 164.508(c), 65 Fed. Reg. 82811-12].
[45 CFR 164.512 (a)].
[45 CFR 164.512 (b)].
[45 CFR 164.512 (c)].
[45 CFR 164.512 (d)].
[45 CFR 164.512 (e)].
[45 CFR 164.512 (f)].
[45 CFR 164.512 (g)].
[45 CFR 164.512 (h)].
[45 CFR 164.512 (i)].
[45 CFR 164.512 (j)].
[45 CFR 164.512 (k)].
[45 CFR 164.512 (l)].
[45 CFR 164.520].
[45 CFR 164.526].
[45 CFR 164.528].
[45 CFR 164.530 (d)].
AIDS Confidentiality Act, 410 ILCS 305/1 et seq.
Alcoholism and other Drug Abuse and Dependency Act, 20 ILCS 301/1 et seq.
Child Care Act of 1969, 225 ILCS 10/1 et seq. (applicable to childcare facilities).
Community Living Facilities Code, 77 Ill. Adm. Code 370.1230 (Confidentiality - adopting the Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).
Confidentiality of Alcohol and Drug Abuse Records, 42 CFR Part 2.

Genetic Information Privacy Act, 410 ILCS 513/1 et seq.
Dental Care Patient Protection Act, 215 ILCS 109/1 et seq. (a patient has the right to privacy and confidentiality).
Early Intervention Services System Act, 325 ILCS 20/1 et seq.
Early Intervention Services System Act Regulations:97
Rules Implementing the Early Intervention Services System Act, 89 Ill. Adm. Code 500.155 (written consent regarding use and exchange of information).
HIPAA Administrative Simplification Regulations, 45 CFR Parts 160, 162), and 164.
Hospital Licensing Act, 210 ILCS 85/6.17 (protection of and confidential access to medical records and information).
Hospital Licensing Regulations, , 77 Ill. Adm. Code 250.1510 (provisions for maintenance, storage, responsibility, content, authentication, verification, confidentiality and security safeguards, indexing and preservation of medical records, and special record requirements for psychiatric service). Note that this law recommends that the unique confidentiality requirements of a psychiatric record, and requires that the unique confidentiality requirements of the alcoholism patient's records, be recognized and safeguarded in any unitized system.
Illinois Constitution, Article I, Section 6 (right to privacy)
Illinois Public Aid Code, 305 ILCS 5/1-1 et seq. (confidentiality and protection of records)
Insurance Code, Article XL, Insurance Information and Privacy Protection, 215 ILCS 5/1001 et seq. (standards for collection, use and disclosure of information gathered by insurers in connection with life, health, disability, property and casualty insurance transactions), including Article XL (Insurance Information and Privacy Protection), 215 ILCS 5/1001 et seq. (standards for the collection, use and disclosure of information gathered in connection with insurance transactions, including medical record information, and restrictions on disclosures without patient authorization and required form of authorization).
Managed Care Reform and Illinois Patient's Rights Act, 215 ILCS 134/1 et seq. (Right to privacy and confidentiality in health care.)
Medical Patient Rights Act, 410 ILCS 50/0.01 et seq. (Patient's right to privacy and confidentiality of records, including restrictions on disclosures by physicians, health care providers, health services corporations and insurance companies.)
Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 (Patient's right to personal privacy and confidentiality of clinical records).
Nursing Home Care Act, 210 ILCS 45/1-1-1 et seq. (privacy and confidentiality of records)
Nursing Home/Long Term Care Regulations: 98
Skilled Nursing and Intermediate Care Facilities Code, 77 Ill. Adm. Code 300.1810 (Resident Record Requirements), 300.1820 (Content of Medical Records), 300.1840, 300.3320 (Confidentiality).
Sheltered Care Facilities Code, 77 Ill. Adm. Code 330.1710 (Resident Record Requirements),

330.4320 (Confidentiality).
Illinois Veterans' Homes Code, 77 Ill. Adm. Code 340.1800 (Resident Record Requirements), 340.1840 (Confidentiality of Resident's Records).
Intermediate Care for the Developmentally Disabled Facilities Code, 77 Ill. Adm. Code 350.1610 (Resident Record Requirements), 350.1630 (Confidentiality of Resident's Records).
Long Term Care for Under Age 22 Facilities Code, 77 Ill. Adm. Code 390.1610 (Resident Record Requirements), 390.1630 (Confidentiality of Resident's Records), 390.3320 (Confidentiality).
Managed Care Reform and Patient Rights Act, 215 ILCS 134/1 et seq. (right to privacy and confidentiality of records).
Medical Patients Rights Act, 410 ILCS 50/.01 et seq. (right to privacy and confidentiality of records).
Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 (Patients' Rights).
Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1 et seq.
Physician and Patient Privilege, 735 ILCS 5/8-101.
Rules Implementing the Community Services Act, 59 Ill. Adm. Code 132.20 (adopting Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).
Rules Implementing the Respite Program Act, 89 Ill. Adm. Code 220.100
Standards and Licensure Requirements for Community Integrated Living Arrangements, 59 Ill. Adm. Code 115.250 (Individual rights and confidentiality - adopting Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).
Workers' Compensation Act, 820 ILCS 305/1 et seq.
http://www.cdc.gov/privacyrule
http://www.hhs.gov/ocr/hipaa
http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html