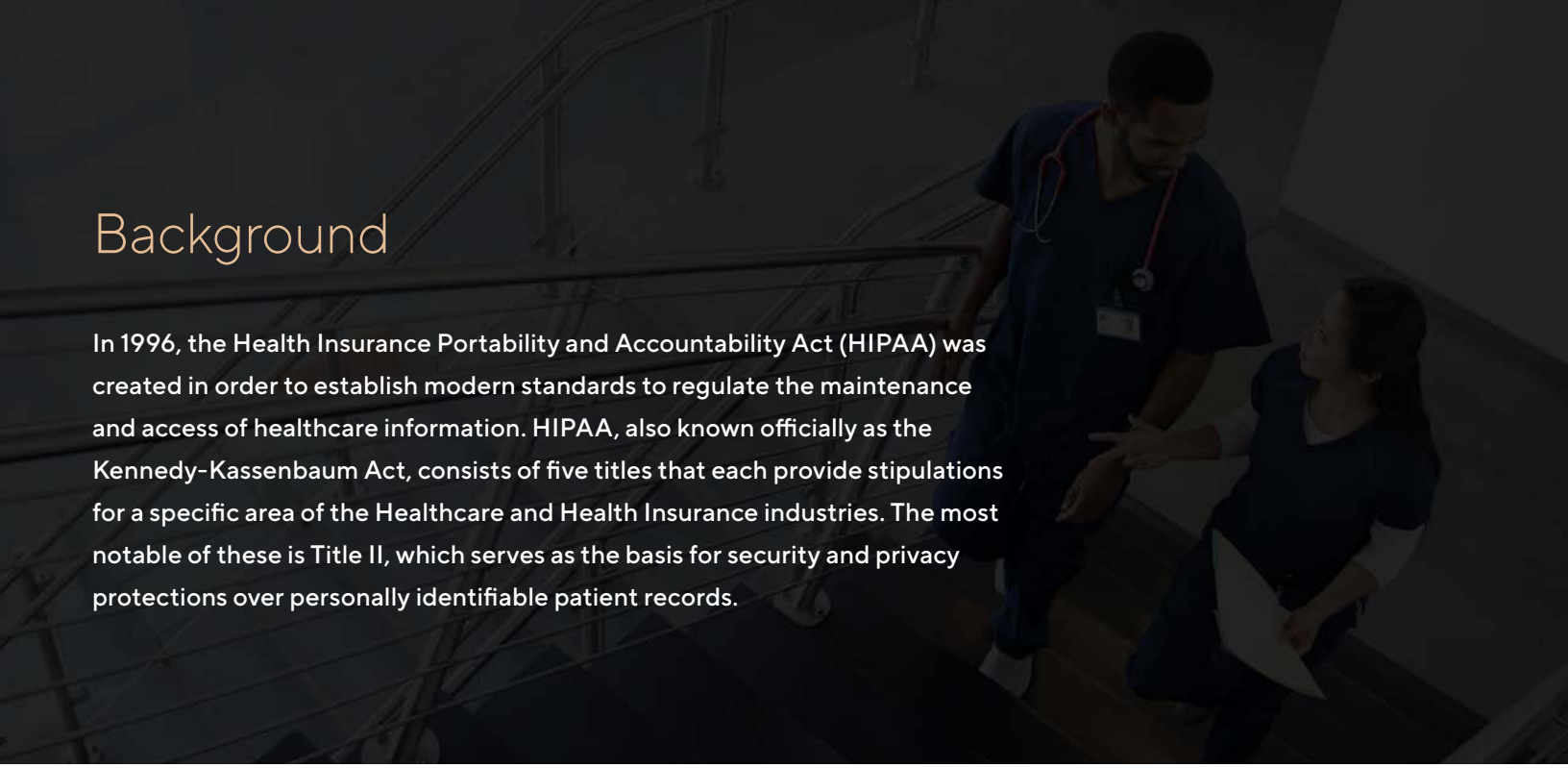
VERKADA

Becoming HIPAA Compliant with Verkada



Background

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was created in order to establish modern standards to regulate the maintenance and access of healthcare information. HIPAA, also known officially as the Kennedy-Kassenbaum Act, consists of five titles that each provide stipulations for a specific area of the Healthcare and Health Insurance industries. The most notable of these is Title II, which serves as the basis for security and privacy protections over personally identifiable patient records.

Who must comply with HIPAA?

The Department of Health and Human Services stipulates that HIPAA must be followed by all "covered entities" including:

- Healthcare Providers (including hospitals, medical centers, clinics, physicians, pharmacies, and nursing homes)
- Health Plans (including company health insurers, health plans, health maintenance organizations (HMOs), and government programs that pay for healthcare)
- Healthcare Clearinghouses
- Business Associates who sign a specific legal agreement with one of these organizations (Verkada is an example of a Business Associate, see below)

How is HIPAA enforced?

HIPAA is enforced primarily by The Department of Health and Human Services Office for Civil Rights (OCR). The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 extends similar investigative authority to the State Attorneys General. Upon receiving a complaint or report of a security breach, the OCR begins conducting an investigation or general audit depending on the severity and specificity of the violation.

When the investigation or audit concludes, OCR determines if any HIPAA regulations were infringed upon and provides assistance in reestablishing compliance if necessary. Serious cases of noncompliance can result in punitive action including financial penalties and potentially even criminal charges if the neglect is provably willful. Violation penalties can total up to $1.5 Million per year if noncompliance remains unaddressed within 30 days of discovery.

HIPAA Violation Penalties

TIER 1	$100 – $50,000 per violation Maximum $25,000 per year	Unaware of the HIPAA violation and by exercising reasonable due diligence would not have known HIPAA Rules had been violated
TIER 2	$1,000 – $50,000 per violation Maximum $100,000 per year	Reasonable cause that the covered entity knew about or should have known about the violation by exercising reasonable due diligence
TIER 3	$10,000 – $50,000 per violation Maximum $250,000 per year	Willful neglect of HIPAA Rules with the violation corrected within 30 days of discovery
TIER 4	$50,000 per violation Maximum $1.5 million per year	Willful neglect of HIPAA Rules and no effort made to correct the violation within 30 days of discovery

Title II - The Administrative Simplification Provisions

Title II of HIPAA codifies rules for maintaining the security and privacy of individually identifiable health information. These provisions, known as the Administrative Simplification rules, require the Department of Health and Human Services (HHS) to establish specific standards for the protection and use of healthcare information. Accordingly, the HHS created a number of rules that have become the basis for what most refer to as HIPAA compliance.

The Privacy Rule

Since the adoption of HIPAA, the HHS has established a number of regulations for the access and disclosure of Protected Health Information (PHI). These regulations are collectively known as Standards for Privacy of Individually Identifiable Health Information, or simply "The Privacy Rule."

Is surveillance footage considered protected health information?

In some cases, yes.

While Protected Health Information usually refers to secure records such as medical history and payment information, the HHS defines it as "individually identifiable health information [...] in any form or media, whether electronic, paper, or oral." So, generally speaking, if footage can be used to directly identify an individual and their treatment, it must be protected under Title II of HIPAA. This could include footage from a patient's room or from another treatment area such as an operating room.

Footage of common areas such as entranceways, waiting rooms, or storage closets are thus not considered PCI and can be shared or stored with fewer restrictions.

www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

The basic tenet of this rule is defined by the HHS: "A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing." Cases where PHI can be disclosed are listed for reference on the HHS website.

In 2009, Title II was amended by the HITECH Act to extend to Business Associates who handle PHI as well. Previous to this, only Covered Entities themselves were required to adhere to HIPAA regulations.

The Security Rule

In order to protect and ensure the privacy afforded to patients by the Privacy Rule, the HHS published the Security Standards for the Protection of Electronic Protected Health Information, also referred to as "The Security Rule." As the title implies, the Security Rule extends protections of the Privacy Rule to records that are stored and transferred electronically rather than physically.

From the HHS website: "The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that [Covered Entities] must put in place to secure individuals' electronic protected health information (e-PHI).

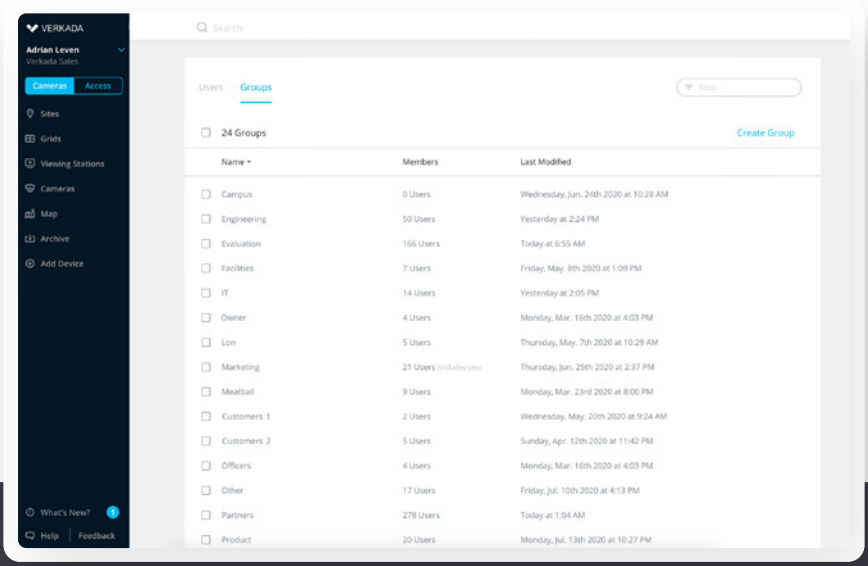
Specifically, Covered Entities and their Business Associates must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures
4. Ensure compliance by their workforce

Verkada's Approach to HIPAA Compliance

The Security Rule lists a number of safeguards to guide organizations in how they manage and protect data. As a Business Associate, the Verkada solution is designed specifically with features that comply with each.

Administrative Safeguards



Security Management Process [45 C.F.R. § 164.306(e)]

A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Verkada Surveillance and Access Control systems can be used to actively monitor secure sites where e-PHI is accessed or stored.

Verkada performs frequent security audits of its storage and transfer of e-PHI. Read more about Verkada Security at www.verkada.com/security

---

Security Personnel [45 C.F.R. § 164.308(a)(2)]

A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Verkada employs a staff of Cloud Security officials who regularly deploy updates to the security of e-PHI storage.

Information Access Management
[45 C.F.R. § 164.308(a)(4)(i)]

Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access)

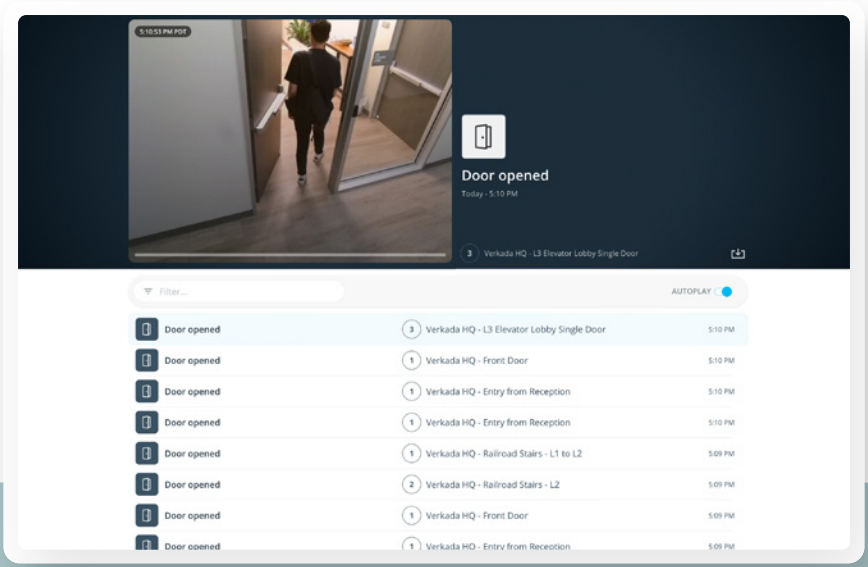
Verkada Command features Role Based Access Control (RBAC), allowing for "minimum necessary" permissions granted on the individual and organizational level.

Information Access Management
[45 C.F.R. § 164.308(a)(4)(i)]

A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Verkada systems are simple to set up and operate, allowing for minimal time invested in training personnel on its use.

Physical Safeguards



Facility Access and Control [45 C.F.R. § 164.310(a)]

A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

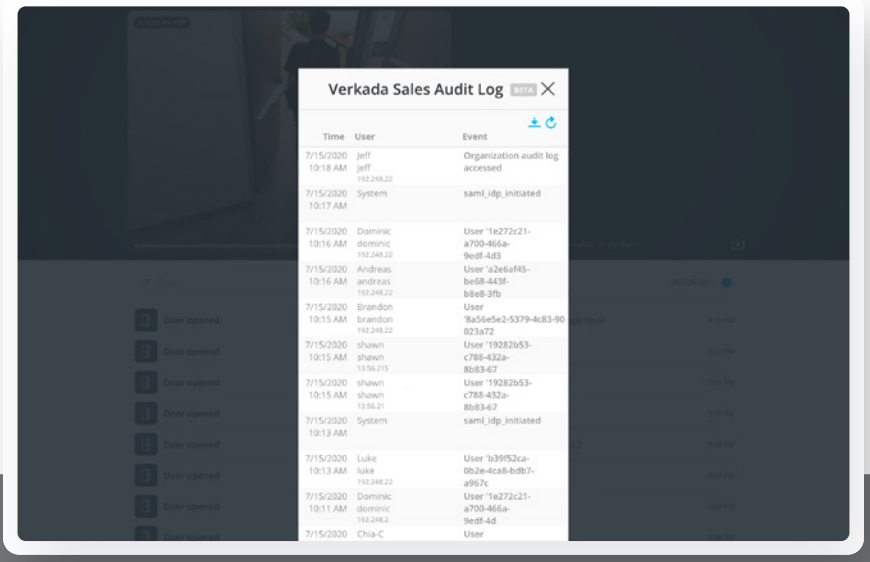
Verkada Access Control makes it easy to assign physical access to only the right parties. Tiered, role-based permissions simplify the process of giving new users the correct level of access.

Workstation and Device Security [45 C.F.R. § 164.308(a)(2)]

A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Verkada Cameras and Access Control can be installed in key locations such as workstations to actively monitor how they're being used.

Technical Safeguards



Access Control
[45 C.F.R. § 164.312(a)]

A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Verkada partners with the most trusted Single Sign-On identity providers in the industry. Traditional Multi-Factor Authentication is available as well.

Audit Controls
[45 C.F.R. § 164.308(a)(2)]

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Verkada Command features comprehensive audit logs that record the identity of anyone who has accessed the system and any changes that they have made.

Integrity Controls
[45 C.F.R. § 164.312(c)]

A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Verkada data is stored redundantly across multiple local AWS servers. Even in the unlikely event that one data center is compromised or disabled, e-PHI will be preserved.

Transmission Security
[45 C.F.R. § 164.312(E)]

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network

All Verkada data is encrypted in transit using the AES 128 and TLS v1.2 algorithms. Whether footage is being sent to the cloud or accessed by a mobile device, e-PHI is safe from unauthorized interception.

Verkada is trusted by over 250 Healthcare Organizations

Affinity Health Plan
BayMark Health Services
Benefis Health System
Chapters Health System
CityMD
ECRMC
Frontier Behavioral Health
Halifax Health
hoag
Indiana Donor Network
Mental Health Center of Denver
St. Charles Health System
UnitedHealth Group
Volunteer Behavioral Health
The Wright Center

Want to Learn More about our HIPAA compliant solution?

Get a Free Trial