Demonstrating HIPAA Compliance

Veriato

www.veriato.com

The biggest challenge in ensuring HIPAA data security is people.

At its core, HIPAA compliance is simply about maintaining patient privacy by ensuring the appropriate access to and use of patient data by your users. Electronic Health Record (EHR) solutions provide detail around when patient data is accessed, but without visibility into what users do with sensitive patient data after they access it, the risk of data breaches, compliance violations, and the investigations, fines, and reputational damage that comes with them, is significantly increased.

Malicious users whose loyalty no longer aligns with the organization can improperly access, copy, email, share, or print patient data – in many cases, without the knowledge of the EHR platform in use.

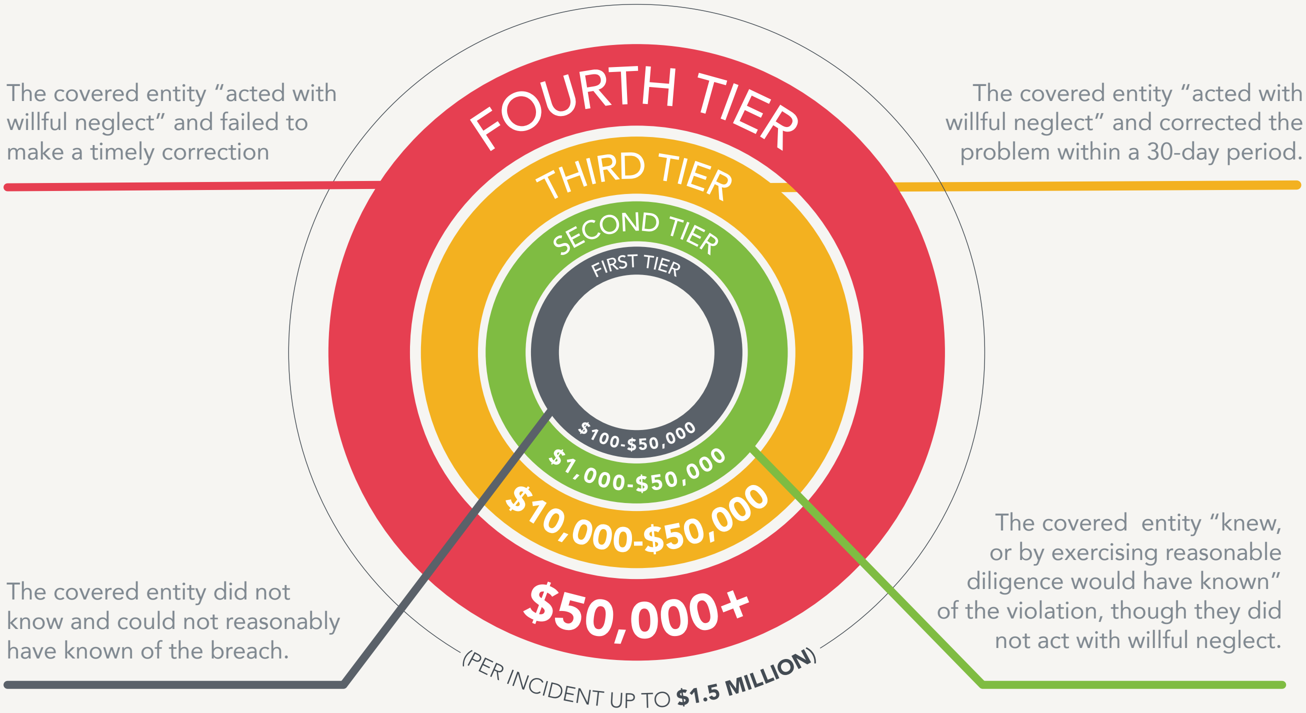
Veriato provides contextual user activity detail and screen recordings necessary to satisfy HIPAA requirements. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that will satisfy the evidence requirements of even the most scrutinizing auditor.

This brief discusses the challenges of safeguarding patient data, and how Veriato uniquely creates the audit detail necessary to meet HIPAA compliance objectives.

Introduction

Organizations seeking to meet HIPAA requirements are expected to demonstrate proper use of patient data through appropriate administrative and technical safeguards. While most organizations focus their efforts on implementing safeguards that revolve around an EHR system already designed to be HIPAA compliant, today's computing environments facilitate the ability to repurpose accessed patient data in an unauthorized fashion, quickly, easily, and conveniently. Webmail, cloud-based storage, USB storage, web-based collaboration tools, and even printing are just some of the ways users can improperly save, steal, and share patient data – making the watching of activity only within an EHR a shortsighted strategy, if the goal is to truly be able to demonstrate compliance.

HIPAA VIOLATION PENALTY TIERS



The covered entity "acted with willful neglect" and failed to make a timely correction

The covered entity "acted with willful neglect" and corrected the problem within a 30-day period.

The covered entity did not know and could not reasonably have known of the breach.

The covered entity "knew, or by exercising reasonable diligence would have known" of the violation, though they did not act with willful neglect.

The penalties for a breach are severe – ranging from hundreds of dollars per record, up to $1.5 million, depending on the tier of the infraction. Avoiding these penalties depends solely on an organization's ability to ensure proper controls are in place, and that access to patient data is proper.

So, what's needed is a means to have complete visibility into every action performed by a user with access to patient data – every application used, webpage visited, record copied, file saved, printscreen generated, and page printed. Only then will a covered entity truly know whether patient data has been appropriately accessed and used.

But, compliance to HIPAA isn't just a technical battle; it's one filled with policies and procedures that, in conjunction with technology, ensure users are trained, access to patient data is correctly granted, use is appropriate, and compliance can be demonstrated.

HIPAA Challenges for Key Stakeholders

While HIPAA itself isn't broken out into separate objectives for each stakeholder in the organization, stakeholders each have different needs around the goal of adhering to HIPAA:

CEO – Needs a proactive approach leveraging people, processes, and technology that ensures adherence to HIPAA requirements around safeguarding patient data.

CFO – Can't afford the cost of a breach in compliance. Would rather spend budget on preventative measures, than on responding to a breach.

CCO – Wants a plan in place of how to easily and quickly demonstrate compliance.

CSO – Desires for patient data to remain secure, and a way to know patient data isn't being misused.

IT Manager – Needs to provide a means of visibility into exactly how patient data is used, regardless of application.

What's needed is a technology that cost-effectively addresses HIPAA requirements by monitoring the access to patient data, aligning with established policy and processes, providing visibility into how patient data is used or misused, and providing context around either demonstrating compliance or determining the scope of a breach

How Veriato Helps Address HIPAA Challenges

Veriato helps organizations of all kinds satisfy their HIPAA obligations through detailed, contextual, rich logging of all user activity – both inside an EHR as well as any other application – combined with robust screen recording and playback. This level of visibility into user interaction with patient data provides comprehensive evidence for compliance audits. Activity data is searchable, making it easy for an auditor, security teams, or IT to find suspect actions, with the ability to playback activity to see before, during, and after the activity in question. Reports can be produced in minutes – typically a fraction of the time needed – and don't require pulling critical resources from other tasks.

Veriato assists in meeting a number of specific requirements, leveraging its deep visibility into user activity to provide context around access to patient data, showing what was accessed and what was done with the data. The following sections outline how Veriato can assist with meeting specific HIPAA requirements.

✓ REQUIREMENT 164.312

Technical Safeguards

Veriato's advanced user activity monitoring and behavior analysis technology can be leveraged to define advanced policy and procedures designed to establish and ensure patient data remains protected.

Below are some examples of how Veriato can assist in addressing some of HIPAA's Technical Safeguards:

- ✓ **Audit Controls (Required)** 164.312(b) – Veriato not only empowers security teams to record an examine user activity within systems containing protected patient data, but also within any other application, providing unmatched visibility into actions taken around patient data access.

- ✓ **Mechanism to Authenticate Electronic Protected Health Information (Addressable)**
 164.312(c)(2) – Because Veriato records and can playback all user activity involving protected patient data, it provides the ability to demonstrate that patient data has not been altered or destroyed in an unauthorized manner.

✓ REQUIREMENT 164.414

Administrative Requirements & Burden of Proof

In an organization's time of need, when demonstrating either compliance – or the lack thereof – is necessary, the determining factor will ultimately be the answer to the question "Was patient data improperly used?". This will require an ability to review the exact actions taken by one or more users, both within and outside of an EHR application.

Below are some examples of how Veriato can assist in addressing this HIPAA requirement:

✓ **Administrative Requirements** 164.414(a) – Veriato's ability to record, playback, and report on detailed user activity can help demonstrate compliance with the Safeguards portion of the Administrative Requirements.

✓ **Burden of Proof** 164.414(b) – In the event of a suspected breach, Veriato uniquely facilitates the playback of specific user activity to either demonstrate the lack of a breach, or to help define the scope of one.

✓ REQUIREMENT 160.308

Compliance Reviews

Whether as part of suspected violation or other circumstances, compliance reviews of administrative provisions around appropriate access to, and usage of, patient data can be simplified by demonstrating enforcement of policies and procedures through Veriato's activity reports and activity playback. .

Demonstrating HIPAA Compliance with Veriato

HIPAA's intent is to ultimately ensure the privacy of patient data. And, as long as the only access to a given patient record is performed by someone who both has a legitimate need and only uses that information for the purposes of the organization, your organization will remain compliant. But, because users with access to patient records utilize that access every day, it becomes nearly impossible to tell if and when your organization may be out of compliance. Add to that the fact that, while the access to a record may seem appropriate, the cutting and pasting of information into a Word doc saved up on a cloud drive certainly isn't – which means your organization needs to be monitoring and recording all user activity, regardless of application.

Veriato assists with establishing compliance with HIPAA requirements by providing IT, security teams, and auditors alike with complete visibility into every action taken by the organizations users. Veriato solutions help to analyze risk, audit controls, and review activity in an effort to establish, maintain, and continually demonstrate HIPAA compliance.

To learn more about how Veriato can help you with HIPAA Compliance, contact a Veriato representative today

8
out of 10

Health

Our solutions are deployed in 110+ countries

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL   United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/