WHITEPAPER

How to Tackle HIPAA Compliance with MDR

Contents

INTRODUCTION

The U.S Department of Health and Human Services (HHS) implemented The Health Insurance Portability and Accountability Act (HIPAA) in 1996 to help modernize and protect privacy and the flow of healthcare information[1].

HIPAA requirements are designed to help support the confidentiality and integrity of electronic protected health information (ePHI), reduce healthcare fraud and abuse, and mandate industry-wide standards for healthcare information on electronic billing and other processes.

Healthcare information and the way it is handled, however, has transformed dramatically over the last decade. Clinics and hospitals currently use digital systems to store and transmit ePHI, and industry professionals and providers now utilize electronic health records (EHR) and other software to digitally maintain sensitive patient data.

The nature of healthcare data, unfortunately, makes it an especially attractive target for cyber criminals. The sheer quantity of information — like the endless pages of forms you must fill out when visiting a doctor – is enticing. No other industry requires that amount of data. The information given is also quite valuable: Social security numbers, payment information, bank accounts, addresses and abundant PII.

Clinics and hospitals also need to maintain a complex array of interconnected legacy and modern systems to keep track of that information. This commonly includes devices and software for managing patient electronic health records (EHR), virtually prescribing medicine, and facilities management systems such as smart heating, ventilation, and air conditioning (HVAC). All these can present unique and high-risk attack vectors for attackers to leverage.

Many healthcare organizations may also be surprised to learn how much of their clinical operations have moved into IoT land: refrigerators, ultrasound machines and other medical devices, Alexa® as a surgery assistant, video cameras, etc.

In addition to all of the devices on their network, healthcare organizations generally have a very porous network perimeter, with VPNs to technology providers, other healthcare providers, insurance companies, EHR providers, etc. This "open door" network concept is a driving factor behind the need for protection with services like Managed Detection and Response (MDR) (more on that later).

Data protection and transmission rules under HIPAA are constantly evolving, and proactive protection is critical. This white paper serves to break down important elements of HIPAA and provide a closer look at the challenges faced by healthcare organizations maintaining or implementing HIPAA compliance for data protection.

Read this guide for a comprehensive introduction to data protection rules mandated under HIPAA—and find out how Bitdefender Managed Detection and Response can help you tackle healthcare compliance like a pro.

Challenges And The True Cost Of Non-Compliance

HIPAA compliance can be overwhelming, especially since technology complexity and diversity have grown (and is growing) exponentially fast. Technology advancements have played an integral part in the evolution and growth discussed in the introduction of this eBook. Traditional measures may have once been enough to adequately protect data in the critical healthcare industry, but security requirements have grown so complex that, in many cases, they've become unmanageable.

Being diligent and proactive is required to successfully and continuously demonstrate compliance.

If you fail to safeguard ePHI as a HIPAA business associate, you can be fined directly for HIPAA violations by the Health and Human Service's Office for Civil Rights, State Attorneys General, and other regulators. Criminal charges may also be applicable for some violations.

The penalty structure for a violation of HIPAA laws is tiered, based on the knowledge a covered entity had of the violation. The Office of Civil Rights (OCR) sets the penalty based on a number of "general factors" and the seriousness of the HIPAA violation.

"Bitdefender MDR assures me that someone is watching our entire network in real-time, including when my staff and I are not in the office. We're able to protect our information assets regardless of where employees are logging in from. MDR is an extension of my team to support the mission of the Archdiocese."

IT Director
Archdiocese | Non-profit | USA

The four categories used for the penalty structure are as follows:

→ **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules

→ **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)

→ **Tier 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation

→ **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

HIPAA Violation Penalty Structure

Each category of violation carries a separate HIPAA penalty. It is up to OCR to determine a financial penalty within the appropriate range. OCR considers a number of factors when determining penalties, such as the length of time a violation was allowed to persist, the number of people affected, and the nature of the data exposed. An organization's willingness to assist with an OCR investigation is also taken into account. The general factors that can affect the amount of the financial penalty also include prior history, the organization's financial condition, and the level of harm caused by the violation.[2]

→ **Tier 1:** Minimum fine of $100 per violation up to $50,000

→ **Tier 2:** Minimum fine of $1,000 per violation up to $50,000

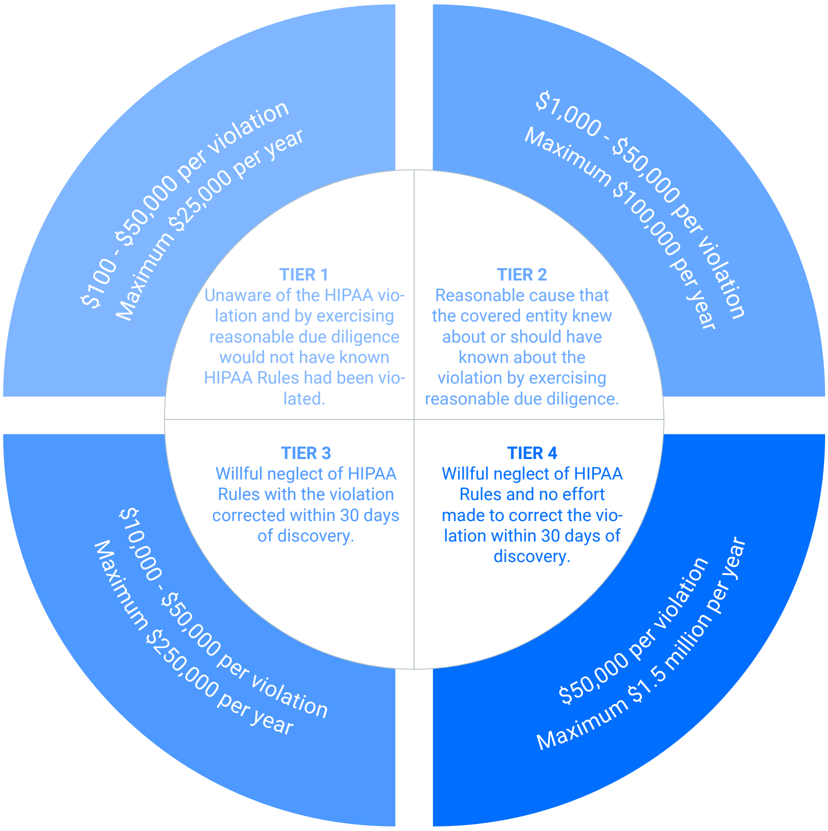
→ **Tier 3:** Minimum fine of $10,000 per violation up to $50,000

→ **Tier 4:** Minimum fine of $50,000 per violation

The above fines for HIPAA violations are those stipulated by the HITECH Act.[3] It should be noted that these are adjusted annually to take inflation into account.

With the latest inflation increases and those applied in previous years, the minimum and maximum HIPAA violation penalty amounts are now as follows:

Penalty Tier	Culpability	Minimum Penalty per Violation – Inflation Adjusted	Max Penalty per Violation – Inflation Adjusted	Maximum Penalty Per Year (cap) – Inflation Adjusted
Tier 1	Lack of Knowledge	$120	$60,226	$1,806,757
Tier 2	Reasonable Cause	$1,205	$60,226	$1,806,757
Tier 3	Willful Neglect	$12,045	$60,226	$1,806,757
Tier 4	Willful Neglect (not corrected within 30 days)	$60,226	$1,806,757	$1,806,757



$100 - $50,000 per violation
Maximum $25,000 per year

TIER 1
Unaware of the HIPAA violation and by exercising reasonable due diligence would not have known HIPAA Rules had been violated.

$1,000 - $50,000 per violation
Maximum $100,000 per year

TIER 2
Reasonable cause that the covered entity knew about or should have known about the violation by exercising reasonable due diligence.

$10,000 - $50,000 per violation
Maximum $250,000 per year

TIER 3
Willful neglect of HIPAA Rules with the violation corrected within 30 days of discovery.

$50,000 per violation
Maximum $1.5 million per year

TIER 4
Willful neglect of HIPAA Rules and no effort made to correct the violation within 30 days of discovery.

The Cost of Non-Compliance

The largest healthcare data breach of 2021 experienced by a HIPAA-covered entity was a hacking incident at the Florida health plan, Florida Healthy Kids Corporation (FHKC). Reported in January 2021, the breach was due to the failure of a security vendor to apply patches to fix multiple vulnerabilities on the FHKC website over a period of 7 years. This basic lack of cyber hygiene allowed hackers to access the website for several years—and they stole highly sensitive information, such as Social Security numbers and financial data. Some of the data on the website was also tampered with. The analysis of the breach revealed the personal and protected health information of 3.5 million individuals was exposed.[4]

The Ohioan Lyon Firm is now actively involved in the security breach and personal data misuse class action lawsuits on behalf of clients of Florida Healthy Kids nationwide.

On July 14, 2022, Oklahoma State University agreed to pay a breach fine for HIPAA violations, including a failure to provide a timely breach notification to affected individuals and U.S. Department of Health and Human Services (HHS) following a hacking incident. In addition to the $875,000 HIPAA breach fine, the university agreed to implement a collective action plan that includes two years of monitoring and oversight.[5]

Hackers first gained access to a web server containing the ePHI of as many as 279,865 individuals on March 9, 2016. The information accessed included patient names, Medicaid numbers, healthcare provider names, dates of service, dates of birth, addresses, and treatment information.

The consequences for failing to proactively follow every HIPAA standard that applies to you are varied and steep, but one thing is for certain: none of them are good.

Data security and active protection are critical to achieving HIPAA compliance; Bitdefender MDR can streamline and simplify the process on your behalf, so you can concentrate on more strategic aspects of your business. Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Protector of millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience.

In fact, Coalfire, a renowned cybersecurity adviser, even awarded our solutions with a flawless HIPAA Compliance Scorecard. Bitdefender received a score of 100% compliance for each of the safeguards and rules evaluated in the extensive Coalfire assessment.[6]

HIPPA Compliance Scorecard

Safeguards and Requirements	Total	No Exceptions	Exceptions	Compliance %
Security Rule				
Administrative Safeguards	28	28	0	100
Physical Safeguards	12	12	0	100
Technical Safeguards	11	11	0	100
Organizational Safeguards	3	3	0	100
Policies and Procedures and Documentation Requirements (1 response(s) empty)	4	4	0	100
Breach Notification Rule				
Breach Notification Rule	5	5	0	100

Bitdefender received a score of 100% compliance for each of the HIPAA safeguards and rules evaluated

DOES HIPAA APPLY TO YOU?

HIPAA applies specifically to “Covered Entities,” which include health plans, healthcare providers and healthcare clearinghouses. It also applies to “Business Associates” that work with those “Covered Entities.” If your business accesses or handles personal patient data (“electronic protected health information” or ePHI) in any capacity, the HIPAA Security Rule is likely to apply.

Covered Entity

A healthcare provider, a health plan, or a healthcare clearing house who, in its normal activities, creates, maintains or transmits PHI. However, most healthcare providers employed by a hospital aren’t considered covered entities. The hospital is considered the Covered Entity and is responsible for implementing and enforcing HIPAA-compliant policies.

Business Associate

A Business Associate is a person or business that provides a service to – or performs a certain function or activity for – a Covered Entity when that service, function or activity involves the Business Associate having access to PHI maintained by the Covered Entity.

Examples of Business Associates include lawyers, accountants, IT contractors, billing companies, cloud storage services, email encryption services, etc. Before gaining access to PHI, the Business Associate must sign an agreement with the Covered Entity stating what PHI they can access, how they plan on using it, and how it will be returned or destroyed once the task mandating it is completed. While the PHI is in the Business Associate´s possession, the Business Associate has the same HIPAA compliance obligations as a Covered Entity.

You can determine whether the Privacy Rule outlined in HIPAA affects you with the covered entities checklist. Covered entities are the people and organizations that hold and process PHI data for their customers and/or patients. Covered entities are also responsible for reporting HIPAA violations, and will be required to pay any fines imposed by the OCR if a HIPAA violation does occur. The Privacy rule protects individual PHI by governing the practice of all covered entities, from doctors and nurses to lawyers and insurance providers.

HIPAA defines these individuals and organizations as covered entities:

→ Healthcare providers

→ Doctors

→ Clinics

→ Psychologists

→ Dentists

→ Chiropractors

→ Nursing homes

- Pharmacies
- Health plan
- Health insurance companies
- HMOs
- Company health plans
- Government-provided health care plans
- Healthcare clearing houses[7]

These entities process healthcare data from another entity into a standard form:

- HIPAA Journal

THE RULES

Security Rule

This requirement consists of three parts: technical, physical, and administrative. The Security Rule contains the standards that must be applied to protect PHI (ePHI) that is electronically created, accessed, processed, or stored – when at rest and in transit. The rule applies to anybody or any system with access to confidential patient data.[8]

Access, in this case, means the ability to read, write, modify, or communicate ePHI, or any personal identifiers that could potentially reveal the identity of an individual.

Privacy Rule

The HIPAA Privacy Rule governs how ePHI can be used and disclosed. Active since 2003, the Privacy Rule applies to all healthcare organizations, the providers of health plans (including employers), healthcare clearinghouses and – as of 2013 – the Business Associates of covered entities.

The Privacy Rule dictates appropriate safeguards be implemented to protect the privacy of PHI. It also sets limits and conditions on the use and disclosure of that information without patient authorization. The Rule also gives patients – or their nominated representatives – rights over their health information, including the right to obtain or examine a copy of their health records and the ability to request corrections.

Under the Privacy Rule, Covered Entities are required to respond to patient access requests within 30 days.

Notices of Privacy Practices (NPPs) must also be issued to advise patients and plan members of the circumstances under which their data will be used or shared.

Covered Entities are also advised to:

- Provide training to employees so they know what information may – and may not – be shared outside of an organization´s security mechanism
- Ensure appropriate steps are taken to maintain the integrity of PHI and the individual personal identifiers of patients
- Ensure written permission is obtained from patients before their health information is used for purposes like marketing, fundraising, or research.
- Ensure their patient authorization forms have been updated to include the disclosure of immunization records to schools, the option for patients to restrict PHI disclosure to a health plan (when they have paid for a procedure privately), and the option of providing an electronic copy of healthcare records to a patient when requested.

Breach Notification Rule

The HIPAA Breach Notification Rule requires Covered Entities to notify patients when there is a breach of their PHI. The Breach Notification Rule also requires entities to immediately contact the Department of Health and Human Services – and issue a notice to the media if the breach affects more than five hundred patients.

Less expansive breaches - those affecting fewer than 500 individuals - also require reporting via the OCR web portal. These smaller breach reports should ideally be made once the initial investigation is complete. The OCR requires these reports be made annually.

Breach notifications should include the following information:

- → The nature of the PHI involved, including the types of personal identifiers exposed
- → The unauthorized person who accessed or used the PHI or to whom the disclosure was made (if known)
- → Whether the PHI was actually acquired or viewed (if known)
- → The extent to which the risk of damage has been mitigated

Breach notifications must be made without unreasonable delay and in no case later than 60 days following the discovery of a breach. When notifying a patient of a breach, the Covered Entity must:

- → inform the individual of the steps they should take to protect themselves from potential harm
- → Include a brief description of actions the covered entity is taking to investigate the breach
- → Detail the actions taken so far to prevent further breaches and security incidents

Omnibus Rule

The HIPAA Omnibus Rule was created to address a number of aspects left unaddressed by previous updates to HIPAA. It amended definitions, clearly outlined procedures and policies, and expanded the HIPAA compliance checklist to cover Business Associates and their subcontractors.

The Omnibus Rule updated HIPAA in five main areas:

- → Introduction of the final amendments as required under the HITECH Act
- → Incorporation of the increased, tiered civil money penalty structure as required by HITECH
- → Introduction of changes to the harm threshold and included the final rule on Breach Notification for Unsecured ePHI under the HITECH Act
- → Modification of HIPAA to include the provisions made by the Genetic Information Nondiscrimination Act (GINA) to prohibit the disclosure of genetic information for underwriting purposes
- → Prevention of the use of PHI and personal identifiers for marketing purposes

Enforcement Rule

The HIPAA Enforcement Rule covers the investigations that follow a PHI breach, potential penalties that could be imposed on covered entities responsible for an avoidable breach of PHI, and the procedures for hearings.

Potential penalties applicable to Covered Entities:

- → A violation due to ignorance can result in a fine of $100 – $50,000
- → A violation that happened despite reasonable vigilance can lead to a fine of $1,000 – $50,000
- → A violation stemming from willful neglect (that is corrected within thirty days) will attract a fine of between $10,000 and $50,000
- → A violation due to willful neglect that is not corrected within thirty days will attract the maximum fine of $50,000
- → Fines are imposed per violation category and reflect the number of records exposed in a breach, the risk posed by the exposure of that data, and the level of negligence involved
- → Penalties can easily reach the maximum fine of $1,500,000 per year, per violation – those identified as willful neglect can also lead to criminal charges being filed. On top of that, civil lawsuits for damages can be filed by victims of a breach

What not to do – the most common disclosures to the department of Health and Human Services:

- **Misuse and unauthorized disclosures of patient records**
- **No protection in place for patient records**
- **Patients unable to access their patient records**
- **Using or disclosing to third parties more than the minimum necessary protected health information**
- **No administrative or technological safeguards for electronic protected health information**[9]

SIMPLIFYING COMPLIANCE

Bitdefender MDR helps you become a more cyber resilient business. We keep you safe with 24x7 security monitoring, advanced attack prevention, detection and remediation, and targeted and risk-based threat hunting from experts that customers can hold accountable. With Bitdefender MDR, you get targeted and risk-based threat hunting by a certified team of security experts focused on your users and systems, while threat intelligence experts keep watch on the outside world, looking for indicators of exposure and data loss.

MDR provides outsourced cybersecurity operations with around-the-clock coverage for customers. Our services combine cybersecurity for endpoints with network and security analytics, underpinned by comprehensive threat intelligence. The Bitdefender MDR Security Operations Center (SOC) is always on, ensuring you are protected and consistently demonstrating HIPAA compliance.

MDR FOR XDR

Managed detection and response (MDR) enhances extended detection and response (XDR) with comprehensive coverage across the organization, ensuring wherever data is stored, threat detection and response is in place.

GravityZone XDR natively observes and detects attacks across an organization’s environment: physical and connected devices, virtual and cloud platforms, and their hosted workloads are all covered.

The GravityZone platform combines advanced threat protection with out-of-the-box analytics, adding a rich security context to the correlation of disparate alerts. This enables security teams to rapidly triage and respond to incidents across identity, network, email, cloud, and endpoints. XDR exposes the full scope of all attacks by connecting events and incidents over time and delivering deeper context through automated evidence collection, root cause analysis, and recommended response actions.

Modern security operations rely on a combination of context, expertise, and intuition to identify malicious activity that can evade your security tools.

GravityZone XDR for MDR enables our security team to analyze and detect intrusions from across your infrastructure with more accurate, correlated detections.

This significantly expands the context available to our cyber threat hunters by providing a more detailed understanding of what ‘normal’ looks like in the environments we defend. In addition, sensors give our analysts access to a suite of additional response actions such as email deletion and user suspension that allows us to take contextual responses to the next level.

GravityZone XDR for MDR is available by adding any sensor(s) to your MDR service: Productivity App, Identity, Network and Cloud.

WHY CHOOSE BITDEFENDER MDR?

Demonstrating HIPAA compliance is a continuous, ongoing process. Bitdefender Managed Detection & Response (MDR) helps keep organizations safe with continuous security monitoring, advanced attack prevention, detection and remediation, and targeted and risk-based threat hunting by a certified team of security professionals.

From small to medium businesses and mid-market to enterprise organizations and mid-market to enterprise organizations can stay one step ahead simply by leaving it to the experts who run our MDR service. Our highly skilled, certified security analysts have experience spanning the U.S. Air Force, U.S. Navy, British Intelligence, and the NSA. They have also created the MDR Cyber Intelligence Fusion Cell (CIFC), which performs extensive monitoring activities to identify company information or high-value employee information that may have been stolen or otherwise leaked. CIFC monitors your domain properties for newly created domains that could indicate “typo-squatting” or URL hijacking behavior by bad actors.

Bitdefender MDR helps ensure organizations have the expertise available to identify threats and respond rapidly to minimize the impact of attacks quickly and effectively – and compliance is a crucial piece of the puzzle. With Bitdefender, you can rest easy, knowing our team of experts is constantly monitoring and evaluating, keeping you protected.

Features and benefits of Bitdefender MDR:

Event monitoring: MDR monitors and investigates all alerts, responds to detections, and provides a detailed analysis via real-time reporting. Analysts run your security operations 24/7 – including human-led threat hunting, environmental baselining, and threat intelligence and analytics – to help you stay ahead of attackers.

Threat hunting: MDR uses tactical and strategic threat intelligence paired with Bitdefender expertise to plan and execute threat hunting missions in the customer's protected environments. Our proactive, highly skilled and certified security analysts, with experience from the U.S. Air Force, U.S. Navy, British Intelligence, and the NSA, partner with you on the frontlines of your cyber defenses.

Pre-approved actions: MDR has a set of documented actions that can be executed in response to findings in the protected environment. Bitdefender knows that some endpoints have an impact on patient care, so PAAs can be tuned so that the Security Operations Center takes action automatically in some cases – and calls the customer first on others.

Review and take action based on alerts: MDR actively reviews alerts from customer environments and proactively assesses telemetry searching for evidence of compromise. MDR then takes specific actions on behalf of the customer to mitigate the business impact.

Reach out to Bitdefender MDR for more info.

About Us

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumers, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

Endnotes

[1] HIPAA for Professionals | HHS.gov
[2] What are the Penalties for HIPAA Violations? 2022 Update (hipaajournal.com)
[3] What is the HITECH Act? 2022 Update (hipaajournal.com)
[4] Florida Healthy Kids website breached; vendor blamed for not patching (databreaches.net)
[5] Oklahoma State University – Center for Health Sciences (OSU-CHS) Resolution Agreement and Corrective Action Plan | HHS.gov
[6] hipaa-privacy-and-security-rule-services (coalfire.com)
[7] HIPAA Compliance and Enforcement | HHS.gov
[8] How OCR Enforces the HIPAA Privacy & Security Rules | HHS.gov
[9] HIPAA Violations, Breaches and Fines | Full List of HIPAA Violations (compliancy-group.com)

Other sources used:

Ransomware Fact sheet https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
hipaa-security-checklist.pdf (healthit.gov)
CNBC http://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html
NIST special Publication http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
Cost of non-compliance: 8 largest data breach fines and penalties - Infosec Resources (infosecinstitute.com)
Healthcare data breaches cost an average $6.5M: report | Fierce Healthcare

HIPAA & Managed Detection & Response: Bitdefender MDR helps you comply with the following Security Standards for the Protection of Electronic Protected Health Information (45 CFR Subpart C)

45 CFR § 164.308 Administrative Safeguards

(a1ii) (a1iiA) ***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 covered entity or business associate.

(a1iiB) ***Risk management*** ✓ **Required.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(a1iiD) ***Information system activity review*** ✓ **Required.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(6i) ***Protection from malicious software*** ☑ **Addressable.** Procedures for guarding against, detecting, and reporting malicious software.

6(ii) ***Log-in monitoring*** ☑ **Addressable.** Procedures for monitoring log-in attempts and reporting discrepancies.

(6ii) ***Implementation specification: Response and reporting*** ✓ **Required.** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

45 CFR § 164.308 - Administrative safeguards. | CFR | US Law | LII / Legal Information Institute (cornell.edu)

(45 CFR § 164.310 Physical safeguards

(b) ***Standard:*** **Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) ***Standard:*** **Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

45 CFR § 164.310 - Physical safeguards. | CFR | US Law | LII / Legal Information Institute (cornell.edu)

§ 164.312 Technical safeguards

(a2b) ***Standard:*** **Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(a2c1) ***Standard:*** **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(a2c2) ***Implementation specification:*** **Mechanism to authenticate electronic protected health information** ☑ **Addressable**. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(e1) ***Standard:*** **Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

45 CFR § 164.312 - Technical safeguards. | CFR | US Law | LII / Legal Information Institute (cornell.edu)

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com