Syteca

E-BOOK

How to Manage Insider Risks in the Healthcare Industry

- Safeguard your PHI and critical systems
- Meet regulatory requirements
- Mitigate insider threats
- Manage third-party cybersecurity risks

www.syteca.com

info@syteca.com

Introduction

The healthcare industry is one of the most vital yet most sensitive in the world - it faces an increase in data breaches year after year. Despite this, healthcare companies continue to digitize patient records and heavily rely on technologies to improve patient care. That's why medical organizations should do their best to ensure their patient data is kept confidential and secure from unauthorized access, cyber threats, and data breaches.

An effective healthcare data security strategy should protect patient healthcare information against theft, alteration, and destruction. It requires implementing robust security practices and policies to safeguard patient data. Healthcare organizations should also address insider threats — one of the most significant risks to healthcare data security.

In this white paper, we explore the main challenges of protecting patient health information against insider threats and offer recommendations on how to prevent and mitigate insider-related incidents through an efficient insider threat program. We also discuss the regulatory landscape and the importance of compliance with relevant laws and regulations.

Source: IBM Security X-Force Threat Intelligence Index 2023
2022 Data Breach Investigations Report | Verizon

Table of contents

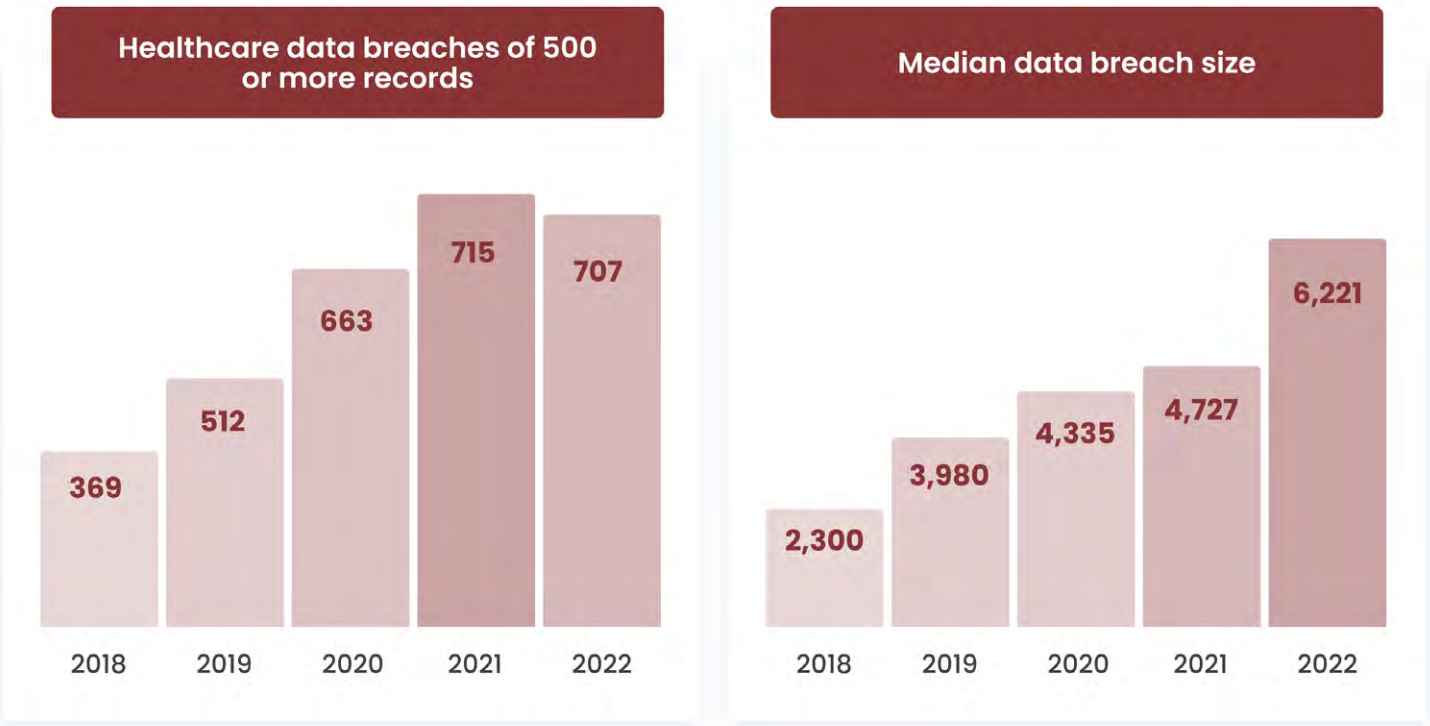
Healthcare data breaches: dangers and challenges

The current situation with healthcare data security is extremely dangerous. There are many cases when patient health information (PHI) is actively sold or used for fraudulent purposes, including opening credit accounts, illegally obtaining prescription drugs, or getting medical services under someone else's name.

Another danger of healthcare data breaches is potential harm to patients' health. Medical records contain sensitive information about patients' health histories, medications, and treatment plans. If this information falls into the wrong hands, it could lead to misdiagnosis, incorrect treatment, or other medical errors.

Such data breaches also present challenges for healthcare organizations, as they can cause reputational damage and result in costly fines, legal fees, and other financial losses. Moreover, after a data breach is detected and investigated, an organization has to spend time and money on assessing and improving their cybersecurity systems.

According to a recent HIPAA report, 5,150 healthcare data breaches of 500 or more patient records were reported to the U.S. Department of Health and Human Services Office for Civil Rights between 2009 and 2022. These breaches led to the exposure of 382,262,109 healthcare records, which equates to more than 1.2 times the US population.



Source: Healthcare Data Breach Statistics (hipaajournal.com)

The exposure of healthcare records leaves millions of patients vulnerable, causing significant financial and emotional harm. Patients may lose confidence in healthcare providers that cannot safeguard their information, which may eventually lead to decreased patient satisfaction and loss of trust.

This is why it's critical for healthcare organizations to prioritize and invest in cybersecurity measures to safeguard patients' sensitive information.

Healthcare data breaches: motives and actors

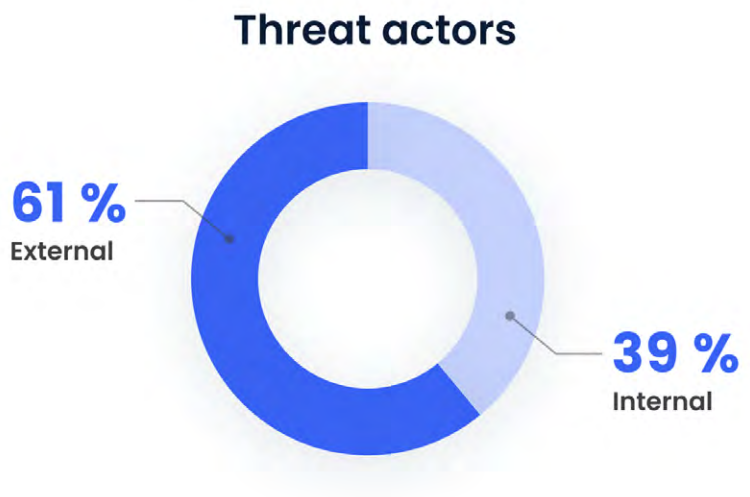
The motives behind healthcare data breaches vary, with threat actors seeking to steal personal information, medical records, credentials, or other records for financial gain or espionage, because they hold a grudge, or for other malicious purposes.

Most sought-after data in 2022	
Personal	58%
Medical	46%
Credentials	29%
Other	29%

Actor motives	
Financial	95%
Espionage	4%
Convenience	1%
Grudge	1%

Source: the Verizon Business 2022 Data Breach Investigations Report (DBIR)

Although the healthcare sector is notorious for insider threats, external threats accounted for 61% of observed threat actors in 2022.



Source: the Verizon Business 2022 Data Breach Investigations Report (DBIR)

While external threats may seem more common, insider threats cannot be overlooked. But before you start to look for the best ways to protect your data from insider threats, you need to understand what dangers they pose.

What are the main types of insiders in the healthcare industry?

As part of a complex industry, healthcare organizations must provide access to sensitive data to a range of parties. Apart from medical staff, this could include hospital management, governmental authorities, insurance managers, etc.

Common examples of insiders in healthcare organizations:

- Physicians, nurses, and other healthcare professionals
- Administrators and executives
- Researchers and academics
- Regulators and government officials
- Third-party vendors and contractors

Not all insiders pose insider threats. But those who cause harm can be categorized depending on their intent. According to the HHS Health Sector Cybersecurity Coordination Center (HC3), the most common types of insider threats to watch out for are the following:

According to the HHS' Health Sector Cybersecurity Coordination Center (HC3)

1. Careless workers

Quite a lot of healthcare breaches result from employees who make honest mistakes or misinterpret HIPAA rules and the organization's policies. These employees are not malicious or intentionally trying to harm the organization, but their lack of awareness and inattention to security policies and procedures can lead to security incidents and data breaches. Careless workers can inadvertently expose sensitive data to unauthorized individuals, compromise critical systems and infrastructure, and disrupt normal business operations.

Examples of careless behavior include leaving a computer unlocked and unattended, using weak passwords, falling for phishing scams, or failing to follow security protocols when handling sensitive data.

To mitigate the risks associated with careless workers, organizations should provide comprehensive security training to all employees as well as implement strong access controls and monitoring systems.

> **While most companies invest more money on insider threats with malicious intent, negligent insider threats are more common.**
>
> *HHS Health Sector Cybersecurity Coordination Center (HC3)*

2. Inside agents

Inside agents are coerced, recruited, or bribed into stealing data, modifying patient records, disrupting healthcare operations, or causing other types of damage. Inside agents could include healthcare professionals, administrative staff, vendors, or third-party service providers.

Inside agents can be stopped by a comprehensive security program that includes access controls, monitoring and auditing systems, incident response plans, and regular security awareness training for all employees. Additionally, background checks, security screenings, and periodic risk assessments can help identify potential insider threats and reduce the likelihood of security incidents.

3. Third parties

Feckless third parties are typically business associates that can compromise security through negligence or harmful access. The dangers posed by third-party insider threats to healthcare

organizations include data breaches, theft of intellectual property, disruption of healthcare operations, and reputational damage. Third-party insiders may intentionally misuse their access to steal data, install malicious software, or disrupt operations. They may also inadvertently cause security incidents by failing to follow security protocols, using weak passwords, or falling for phishing scams.

To mitigate risks, facilities should implement strong access controls and monitor all critical systems. In addition, they should require third-party vendors to undergo regular security assessments and audits.

4. Disgruntled employees

Disgruntled employees are typically individuals who are dissatisfied with their job and may intentionally use their access to the organization's systems or data to cause harm.

The dangers posed by disgruntled employees to healthcare organizations include data breaches, theft of sensitive data, disruption of healthcare operations, and reputational damage. Disgruntled employees may intentionally delete or modify critical data, install malicious software, or send sensitive information to external parties.

Employees may turn into inside actors in their final days in your organization. The most effective way to detect and deter them is to implement strong user behavior monitoring tools that can track and notify about any abnormal behavior and unusual actions.

5. Malicious insiders

Malicious insiders are the most challenging threats to detect. Unlike inside agents, they usually have their own motivations for accessing private information. Malicious insiders often steal patient information to commit identity theft or fraud. Countermeasures to protect your sensitive data against malicious insiders include controlling access, monitoring users for suspicious activity, and restricting the use of USB storage devices. Background checks, security screenings, and periodic risk assessments can also help identify potential insider threats.

6. Compromised insiders

In the last few years, the most common initial attack vector was stolen or compromised credentials. Compromised insiders are individuals within a healthcare organization whose access to sensitive data or systems has been exploited by external threat actors. Compromised insiders may have unwittingly provided their login credentials or been tricked into downloading malware, allowing attackers to get inside the organization's network. Multi-factor authentication and mon-

itoring for unusual activity can help security officers detect compromised users, whereas security awareness training can minimize the risk of stolen credentials.

In October 2021, Broward Health suffered a data breach caused by a third-party medical provider that had access to its patient database.

Impact: 1.3 million patients

Data compromised: Names, addresses, dates of birth, driver's license numbers, insurance information, medical information

What could be done to prevent this accident:

- Implement multi-factor authentication (MFA) across all endpoints
- Implement privileged access management
- Keep track of all endpoints that connect (or attempt to connect) to the private network

What are insider risks in healthcare and their consequences?

Insider risks in healthcare refer to the potential threat that comes from employees, contractors, or other individuals who have access to sensitive patient data, systems, or facilities. These individuals can intentionally or unintentionally misuse or mishandle data, which can cause significant harm to the healthcare organization and the patients they serve.

Main risks and their potential consequences:

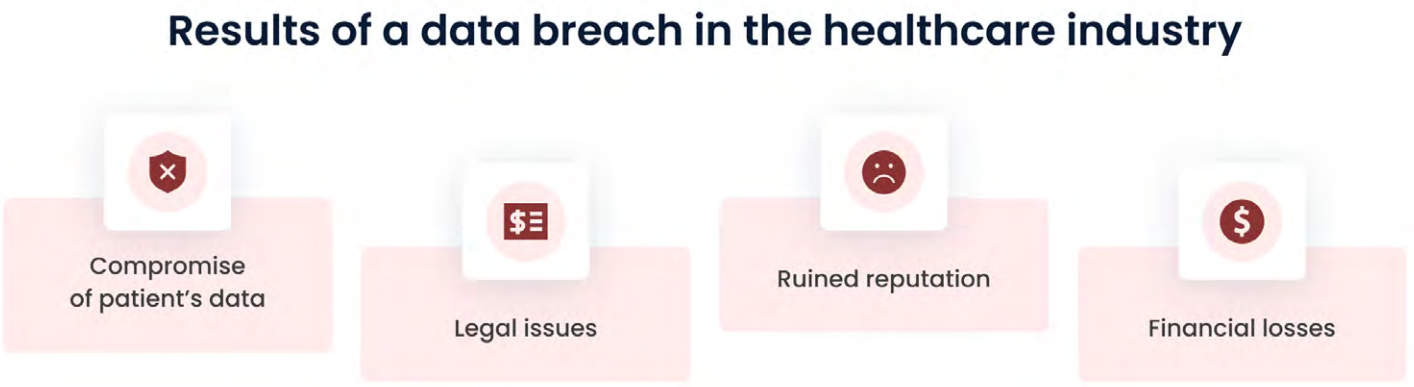
1. **Unauthorized access to patient data.** Insiders may gain access to patient data without obtaining the patient's consent, either by exploiting their privileges or by using stolen credentials. This can result in exposure of sensitive patient information, such as medical history, treatments, and prescriptions, and can lead to a breach of privacy and trust.

2. **Data theft or leakage.** Insiders may steal or leak sensitive patient data for financial gain, personal reasons, or to harm the healthcare organization. This can lead to reputational damage, loss of trust, legal penalties, and financial losses.

3. **Human error.** Insiders may unintentionally cause harm by making mistakes, such as misplacing patient data or sending sensitive information to the wrong recipient. These errors can result in data breaches, privacy violations, and regulatory non-compliance.

4. **Malicious activities.** Insiders may engage in malicious activities such as introducing malware, tampering with patient data, or disrupting critical systems. This can cause significant disruptions to patient care, compromise patient safety, and result in financial losses.

Furthermore, healthcare organizations may face regulatory fines and legal action if they fail to comply with data protection laws and regulations, such as HIPAA.



The cost of data breaches in healthcare

One of the most painful consequences that organizations face is financial losses. Typically, these losses are overwhelming and include various components:

- **Direct costs** associated with the breach, including investigation and remediation costs, notification costs, and legal fees
- **Indirect costs** that arise as a result of the breach (not directly related to the breach itself), which may include lost business opportunities, reputational damage, and, consequently, reduced productivity
- **Regulatory fines and penalties.** As healthcare organizations are subject to various laws and regulations that govern the privacy and security of patient data, they are often subjected to regulatory fines and penalties if data breaches occur
- **Lost revenue**, which may include the loss of patients or customers or the cost of responding to the data breach itself
- **Recovery costs** invested in additional cybersecurity measures to prevent future breaches

The average cost of a healthcare data breach hit a new record in 2022, increasing by almost $1 million to a whopping $10.10 million.

Average cost of a data breach by industry 2021/2022

Industry	2021	2022
Healthcare	$9.23	$10.10
Financial	$5.72	$5.97
Pharmaceuticals	$5.04	$5.01
Technology	$4.88	$4.97
Energy	$4.65	$4.72

(millions USD)

Source: Ponemon 2022 Cost of Insider Threats Global Report

The most alarming part is that when a breach occurs, it's rarely discovered quickly. On average, it takes 277 days to identify and contain a data breach.

> **For 12 years in a row, healthcare remains the most expensive industry in breach costs.**
>
> *2022 Cost of Insider Threats Global Report*
> *by the Ponemon Institut*

Electronic health record systems: benefits and vulnerabilities

Knowing that hacking of healthcare organizations is on the rise leads us to the question of what exactly is lacking in healthcare software and how we can protect sensitive data. Almost all healthcare providers use Electronic Health Record (EHR) systems to store and manage sensitive healthcare data, including the following patient records:

Electronic Health Record (EHR) systems can store and manage

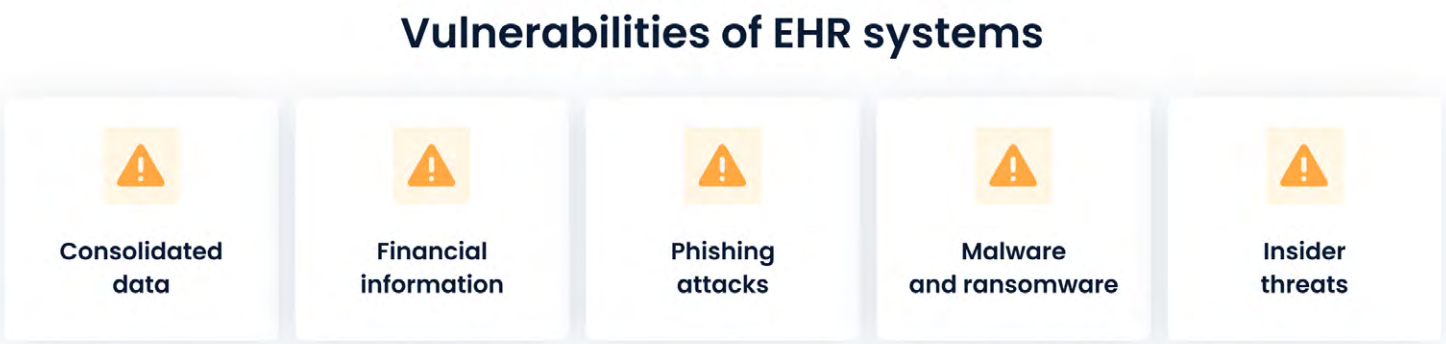
1. Full name and birth date
2. Bank account information
3. Health data
4. Social Security number
5. Insurance information
6. Contact information
7. History of visits to healthcare professionals
8. Hospitalization records
9. Allergies and immunization status
10. Family history
11. List of prescribed medications
12. Medical images

The EHR initiative was born thanks to the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Benefits of EHR systems

- ✓ Streamline workflows
- ✓ Consolidate all data in one place
- ✓ Improve care coordination
- ✓ Automatically update information
- ✓ Reduce healthcare disparities
- ✓ Share media such as medical images
- ✓ Share information among offices and organizations

However, EHR systems have several significant downsides when it comes to healthcare data security:



- **Consolidated data** poses a great security risk. If perpetrators get access to the system, they can get full control over a wide range of personal patient data.
- **Financial information**. Apart from patient records, financial data also attracts cybercriminals.
- **Phishing attacks** may cause severe damage to data security if healthcare professionals aren't taught how to identify them.
- **Malware and ransomware** can reach EHR systems via downloads, software vulnerabilities, and even encrypted traffic. This malicious software may cause harm not only by stealing data but also by locking users out of their computers and demanding payment to regain access.
- **Insider threats** come from medical staff. Employees can cause trouble on purpose (stealing information to sell it) or by accident (disclosing it due to a lack of cybersecurity education).

Why does the current approach have problems?

Most data protection solutions in healthcare are focused on establishing and maintaining a security perimeter, but most attacks and security breaches happen from within the system.

Perpetrators can be either employees or criminals trying to get access to the system from inside the building – for example, by using a public Wi-Fi connection or a USB device.

To protect patient information stored in hospitals and other healthcare organizations from such insider threats, organizations should integrate employee activity tracking solutions into their cybersecurity program. Almost all EHR systems have some user tracking features, allowing you to see who accesses sensitive data. However, such features have their own limitations and vulnerabilities.

- Usually, EHR systems don't record the actions of **users with privileged accounts**, such as administrators. This allows those users to carry out malicious activity undetected.
- Administrators can go undetected when **changing the entitlement level of any user,** including themselves. Thus, they can circumvent internal system monitoring and access personal patient data.
- Even if access to sensitive data is recorded, it's **impossible to know how the data was used**. Therefore, it's complicated to detect malicious actions in time and prove violations.

To overcome all these drawbacks of EHR systems, it's essential to use tracking software that monitors all user activity in compliance with the HIPAA audit checklist. For electronic health record systems, auditing software that provides constant EHR system monitoring can significantly speed up the audit process, lessening your headaches and costs.

The importance of an insider risk management strategy

It's crucial for healthcare organizations to implement an insider risk management strategy to prevent, detect, and respond to insider-related incidents.

1 **Protect sensitive patient data.** Insider risk management can help healthcare organizations safeguard sensitive patient data by identifying and mitigating potential risks. This can prevent unauthorized access to patient data, data theft or leakage, and malicious activities that can compromise patient confidentiality.

2 Comply with IT requirements. Healthcare organizations must comply with various data protection regulations and laws, such as HIPAA in the United States. And as penalties for HIPAA violations can be severe and reach into the millions of dollars, an effective insider risk management strategy is a must. It can help healthcare organizations meet regulatory requirements and avoid fines and legal action for non-compliance.

3 **Maintain patient trust.** Patients should trust healthcare organizations and be sure that they will protect their sensitive health information. By implementing a good insider risk management strategy, healthcare organizations can demonstrate their trustworthiness and commitment to data security.

4 **Enhance cybersecurity.** An effective insider risk management strategy can enhance the cybersecurity posture of healthcare organizations by improving their overall security awareness and readiness. This can lead to faster detection and response to insider-related incidents. Hence, it can minimize the damage caused by data breaches.

9 best practices to manage insider risks in healthcare

To manage insider risks and ensure the security of sensitive data, healthcare organizations need to implement a comprehensive insider risk management program that includes policies, procedures, employee training, and other effective practices.

1. Assess cybersecurity features of the electronic health record (EHR) system

Assessing the cybersecurity features of an EHR system is essential for protecting sensitive information, complying with requirements, and protecting the reputation of the healthcare organization.

- Identify security requirements that your EHR system must meet. These include laws such as HIPAA as well as internal policies and procedures.
- Review the technical specifications of your EHR system to understand how it implements your security features. Review the methods used for encrypting data, access control mechanisms, as well as authentication and authorization mechanisms.
- Conduct a vulnerability assessment to identify any weak points in your EHR system, covering network security, application security, and data security.
- Review compliance of your EHR system with data protection requirements.

2. Implement strict password and account management policies and practices

Implementing strict password and account management policies is important to mitigate insider threats and maintain system availability.

- Establish password policies that require users to create strong, unique passwords that are changed regularly.
- Regularly review and update these policies to keep up with changing security threats and industry best practices.
- Segment your network to reduce the risk of lateral movement by attackers.
- Track the use of USB devices. Besides passwords, you should approve or prohibit certain types of USB devices, then continuously monitor all connected devices via USB device monitoring tools.
- Monitor user behavior. Healthcare organizations should monitor user behavior to detect any suspicious activities, such as unauthorized access attempts or unusual patterns of data access.

3. Limit privileged access and establish role-based access control

Limiting privileged access and establishing role-based access control is crucial for preventing unauthorized access, protecting critical data, and minimizing security incidents.

- Limit access to sensitive information. Use role-based access controls to make sure critical data is available only to those who require access to it.
- Consider giving privileged access only to a narrow circle of employees, and pay close attention to each of them.
- Conduct user access reviews. Healthcare organizations should conduct regular audits of user accounts and access privileges to make sure each role has the right set of permissions.

4. Use the zero-trust and MFA models

Using the zero-trust and MFA models can ensure the security of your digital assets and safeguard your organization against unauthorized access.

- Define access policies. Specify who can access which resources, under what circumstances, and from which devices. Access policies should be based on the principle of least privilege, meaning that users should be granted only the minimum access required to perform their job functions.
- Implement multi-factor authentication (MFA). This is one of the most effective ways to prevent unauthorized access to sensitive information. MFA requires users to provide additional forms of authentication, such as a one-time code sent to a mobile device, in addition to their password.
- Consider implementing a zero trust architecture and a just-in-time privileged access management (PAM) approach.

5. Enhance control over shared accounts

Enhancing control over shared accounts is important because shared accounts can be exploited by insiders and, thus, pose serious security vulnerabilities.

- Monitor third-party users. As healthcare organizations continue to outsource their business functions, third parties can pose significant risks. You should define all outsiders who have access to your systems or data (vendors, contractors, and consultants). Each third-party user should be assigned a unique account that can be properly tracked and monitored.

- Establish user access policies and implement MFA. Just as with regular employees, you should establish strong authentication procedures and user access policies to make sure third-party users are granted access only to the systems and data they require to perform their duties.

- Conduct scheduled security reviews. Healthcare organizations should conduct regular security reviews to ensure that policies and procedures for managing third-party users are up-to-date and effective. This includes reviewing access policies, auditing user activity, and testing the effectiveness of MFA.

6. Review and update cybersecurity policies and guidelines

It's necessary to regularly review and update cybersecurity policies and guidelines because technology and cyber threats are constantly evolving, and outdated policies may not adequately address new threats.

- Conduct a risk assessment. This is a critical step in reviewing and updating cybersecurity policies and guidelines and can help healthcare organizations identify potential threats and vulnerabilities at early stages. Risk assessment should be comprehensive and include an analysis of all aspects of the organization's IT infrastructure, including hardware, software, and data.

- Constantly review industry standards and regulations. To ensure that your cybersecurity policies and guidelines are aligned with the latest best practices, review relevant laws (HIPAA and HITECH) and guidance from organizations such as NIST and HITRUST on a regular basis.

- Identify individuals who are responsible for specific areas of cybersecurity, such as network security, access control, and incident response.

- Establish an incident response plan. Healthcare organizations should establish clear incident response procedures to ensure they can react quickly and effectively to cybersecurity incidents.

7. Educate employees on indicators and risks of data misuse

As employees are often the first line of defense against insider threats, they need to be aware of signs of data misuse and how to report incidents in order to prevent data breaches and protect sensitive information.

- Develop a training program to ensure that all employees understand their roles and respon-

sibilities regarding cybersecurity. Training should cover topics such as password management, phishing awareness, and incident response.

- Raise awareness of the EHR system's security features and policies. This includes training on topics such as data protection and incident reporting.
- Inform employees about the consequences of data misuse to help employees understand the importance of protecting sensitive data and the potential impact of data breaches.
- Provide clear guidelines on how to handle sensitive data and what to do if one suspects data misuse.

8. Develop an insider threat mitigation program

A good insider threat mitigation program can help your organization promptly identify and address potential insider threats, reduce the risk of data breaches and other security incidents, and improve overall security.

- Establish an insider threat team if you don't have one. Your team should manage the program and respond to insider incidents. The team should include representatives from the IT, HR, legal, and compliance departments.
- Conduct thorough background checks on your employees, contractors, and third-party vendors before granting access to sensitive data or systems.
- Integrate dedicated software to detect and prevent insider threats. Your software should let you constantly monitor user activity to detect anomalous behavior and potential insider threats.
- Continuously evaluate and improve your incident response plan and insider threat mitigation program to ensure that they remain effective and up to date with the industry's latest cybersecurity practices and regulatory requirements.

> **Insider threat mitigation programs need to be able to detect and identify improper or illegal actions, assess threats to determine risk levels, and implement solutions to manage and mitigate the potential consequences of an insider incident.**
>
> *CISA*

9. Back up data and deploy data loss prevention tools

By backing up data, an organization can ensure that it can recover patients' records and critical data in the event of a breach or other security incident, reducing its negative impact.

- Identify the types of data that are most critical to the organization, such as patient records, financial information, and intellectual property.
- Define backup and recovery procedures. Develop procedures for backing up critical data, including how often backups should be performed, where backups should be stored, and how backups should be tested for recoverability.
- Deploy data loss prevention (DLP) tools across the organization, including on endpoints, servers, and networks. These tools should be configured to monitor for policy violations and alert security teams to potential data breaches.
- Monitor alerts and respond promptly to potential data breaches. This includes investigating and resolving any policy violations, as well as containing and recovering from data breaches.

> **Healthcare risk managers must adapt and be proactive in developing and implementing initiatives that enhance organizational performance and productivity while improving patient outcomes.**
>
> *American Society for Healthcare Risk Management*

How Syteca helps healthcare organizations prevent insider risks

Syteca helps healthcare organizations prevent insider risks by providing a robust insider threat management strategy. With Syteca, you can monitor user activity in real time, record all user sessions, and generate detailed audit trails. This helps identify suspicious behavior and potential threats quickly. Additionally, Syteca allows organizations to restrict access to sensitive information, limit user privileges, and enforce security policies to prevent unauthorized access.

Syteca also helps healthcare facilities comply with major cybersecurity requirements, such as HIPAA and HITECH, by providing detailed audit logs and reports.

In this section, we briefly overview three cases when healthcare organizations adopted Syteca for enhanced cybersecurity.

Baruch Pada Medical Center secures third-party activities with Syteca →

European healthcare provider protects sensitive data from insider threats using Syteca →

Healthcare organization ensures HIPAA compliance and efficient remote work with Syteca →

Baruch Pada Medical Center secures third-party activities with Syteca

The challenge

The Baruch Pada Medical Center in Israel provides a wide range of healthcare services to people all over the country. And since all vendors have access to the center's computer network, the facility was looking for an efficient way to control this access and, thereby, secure a huge number of medical/personal records of its patients.

- Improve management of third-party access
- Reduce the risk of third-party insider threats
- Ensure the security of sensitive data

The solution

The Syteca platform provided Baruch Pada Medical Center with a comprehensive set of features to monitor and control user activity on critical systems:

- Automated credential management and provisioning
- User groups with flexible configuration of access rights
- Continuous third-party activity monitoring
- Detailed and searchable logs of third-party user sessions
- Real-time alerts on suspicious security incidents
- Cybersecurity threat response and blocking capabilities

The results

By implementing Syteca, Baruch Pada Medical Center managed to:

- Achieve a more secure and reliable IT environment
- Automate and conveniently manage access rights for third-party users
- Gain greater visibility into user activity
- Identify potential insider threats
- Respond quickly to security incidents

> **The load on our IT team was significantly reduced immediately, as all vendors connect to a single IP point, and we can control and monitor where each user connects, as well as make sure they don't move from there to other servers. Second, all the activities of each and every contractor are documented and recorded on video so we can watch past activities and explore and export data, which maximizes the level of information security.**
>
> **Zvika Klinger,**
> *Director of technology,*
> *Baruch Pada Medical Center*

European healthcare provider protects sensitive data from insider threats using Syteca

The challenge

As our customer works with loads of sensitive healthcare data, the company needed to protect it according to their corporate cybersecurity policies and industry requirements. What made things trickier was the fact that the healthcare provider had comprehensive infrastructure with lots of facilities all across Europe, where numerous IT administrators performed cross-system operations. The company turned to Syteca to:

- Establish reliable oversight of healthcare data
- Audit administrators' activity
- Manage access of privileged users
- Maintain a convenient multi-tenant infrastructure

The solution

Syteca enabled the customer to leverage the following functionalities:

- Monitoring of user actions with sensitive data
- Alerts and notifications on suspicious activity
- Searchable records of user sessions
- Exportable user activity reports
- Granular remote desktop (RDP) access control via terminal server
- Floating licensing scheme
- Multi-tenant mode
- Integration with log management (LM) and SIEM systems

The results

By adopting Syteca, the healthcare provider had the opportunity to:

- See who does what with sensitive data
- Respond to insider threats in real time
- Know how privileged users handle sensitive data
- Limit admin access to a particular facility
- Manage server configurations separately for each facility
- Gather and process monitoring data from all facilities in one place

> **The [Syteca] solution from DATASYS helped us gain full control over the activities of privileged users of third-party employees on selected servers and terminals.**
>
> *Cyber Security Manager*

Healthcare organization ensures HIPAA compliance and efficient remote work with Syteca

The challenge

Our client's organization was facing the challenge of managing access to electronic protected health information (ePHI) and preventing unauthorized access to sensitive patient data while effectively monitoring remote employees. In addition, the company had to comply with the Health Insurance Portability and Accountability Act (HIPAA). The company decided to integrate Syteca to:

- Simplify monitoring system maintenance
- Track remote employees' productivity
- Maintain HIPAA compliance

The solution

Syteca helped the organization benefit from:

- Continuous user activity monitoring
- Real-time alerts on suspicious user actions
- Convenient monitoring of remote employee activity and productivity reports
- Easy installation and responsive technical support
- A user-friendly web interface
- Silent updates with no need for operating system reboots

The results

By implementing Syteca, the organization was able to achieve:

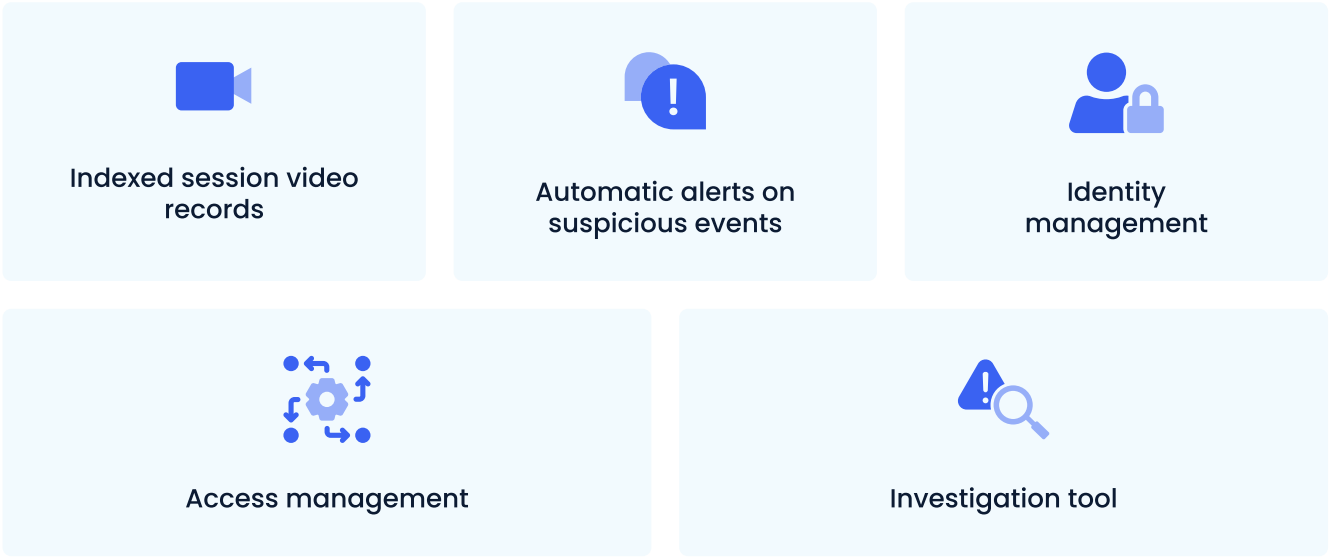
- Full visibility into employee activity
- Fast detection of and response to cybersecurity policy violations
- The ability to analyze employees' performance
- Fast platform deployment
- Quick search for a specific device or user
- Software updates without workflow disruptions
- Compliance with HIPAA security rules

> **We have been using it [Syteca] for almost a year now. I really enjoy being able to see from a web browser the entire state of the system and recording without going onto the server itself. We have seen alerts come across and are able to react quickly to verify what is going on.**
>
> *Network Administration Manager Healthcare Organization*

How can Syteca enhance your cybersecurity?

Syteca provides compliance with various laws, regulations, and standards, including HIPAA. It monitors all user activity on servers and desktops, in applications, on webpages, and on any visible area of the screen.

Syteca secures your healthcare software



As per HIPAA requirements, Syteca provides access control functionality and can help you analyze risk and establish a clearance procedure. You can use Syteca to develop and deploy user activity reviews and implement critical administrative and technical safeguards required by HIPAA. Additionally, Syteca can help you meet compliance requirements established by the PCI Security Standards Council, SOX, NERC, and other laws and organizations, as well as get prepared for almost any IT compliance audit.

Along with ensuring regulatory compliance, Syteca can safeguard your financial data, patient data, and other confidential information thanks to the following features:

- **Indexed session video records.** Syteca records a video of everything a user sees and does on their screen (with configurable quality). A YouTube-like player provides a Live Session View, keyword search, and multilayer metadata, including the name of the current application and opened URLs.
- **Automatic alerts on suspicious events**. The user and entity behavior analytics (UEBA) module in Syteca uses an alert system and an artificial intelligence module to detect

suspicious activity and alert you immediately. This feature also supports USB management: Syteca logs USB device connections, alerts on connected devices, and blocks them with rules, whitelists, and blacklists.

- **Identity management**. Syteca identifies all users with a secondary level of authentication, allowing you to distinguish between users who work under shared accounts. Two-factor authentication is employed for all users, including privileged ones.
- **Access management.** Syteca provides privileged account and session management (PASM) to help you monitor and review all activities carried out by a privileged user, configure who can access what endpoints within a protected perimeter, and set expiration and update dates for credentials.
- **Third-party monitoring.** Syteca allows for setting granular access control for third-party users and performing third-party identity verification to make sure your sensitive data doesn't get into the wrong hands. Meanwhile, real-time alerts and activity reports further enhance third-party management.
- **Investigation tool functionality.** Broad reporting tools summarize various aspects of data, including all user logins for an endpoint, visited URLs, and the most and least used applications. You can painlessly export recorded sessions, episodes, and other results of a cybercrime investigation in a forensic format.

Using Syteca, you can monitor and record sessions of all users, including privileged and third-party users, so you can further review any access to and actions performed on sensitive data. Moreover, Syteca provides an access policy and report tools to extract evidence if needed by investigators.

The features offered by Syteca allow you to know precisely who has access to patient data and how they're using it. These features can be used to organize a timely incident response, prevent identity theft and fraud, and provide evidence in case of a criminal investigation.

Final thoughts

Protecting patient health information is crucial for the healthcare industry, as patient data security breaches can have severe consequences. Implementing robust security measures, policies, and procedures is necessary to safeguard patient data and prevent unauthorized access, cyber threats, and data breaches. Healthcare organizations must also address insider threats, which are a significant risk to healthcare data security.

It's crucial for healthcare organizations to enhance their cybersecurity with robust insider threat protection software. By doing so, you can not only safeguard your patient privacy and prevent financial losses but also ensure regulatory compliance and maintain your reputation as a trustworthy provider of quality care.

Syteca provides comprehensive solutions to secure healthcare software, including compliance with HIPAA requirements, access control, risk analysis, identity management, and privileged account and session management. The software also features automatic alerts on suspicious events, user and entity behavior analytics, and investigation functionality, providing healthcare organizations with the necessary tools to monitor and review all activities carried out on sensitive data.

In short, Syteca can:

- Protect access to EHR systems
- Secure your patients' personal data
- Track third parties and software service providers
- Ensure proper HIPAA compliance
- Be easily deployed on both a small and large number of endpoints and servers

All these features can help organizations prevent fraud and identity theft and provide evidence in case of a criminal investigation.

Syteca can significantly contribute to healthcare data security and ensure the utmost protection of sensitive data.

Protect your sensitive data using Syteca

Visit www.syteca.com or email us at info@syteca.com

Syteca

About us:

Syteca is a cybersecurity platform with rich functionality for privileged access management and user activity monitoring. By leveraging the Syteca platform, you can strengthen your cybersecurity and effectively manage human-related risks.