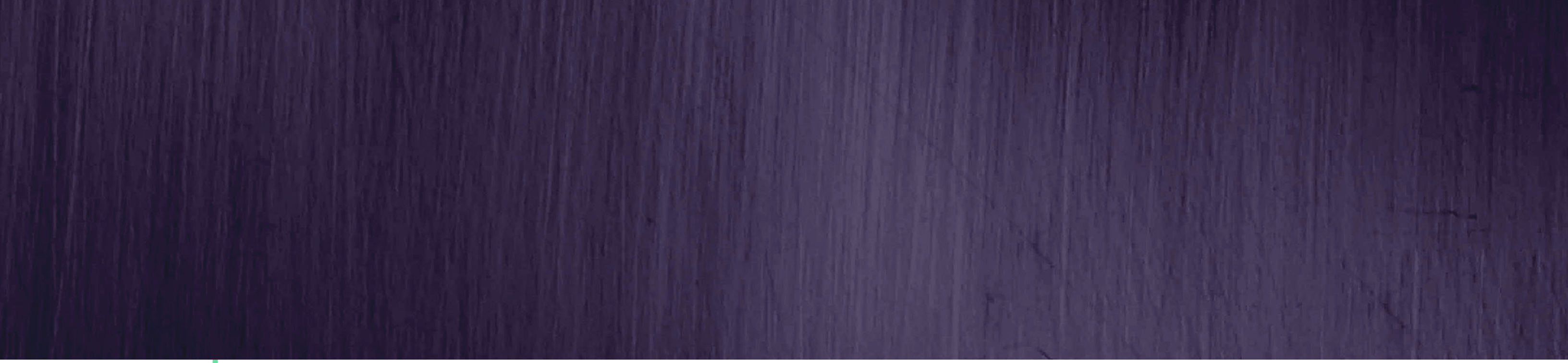
Data Protection Guide for Healthcare

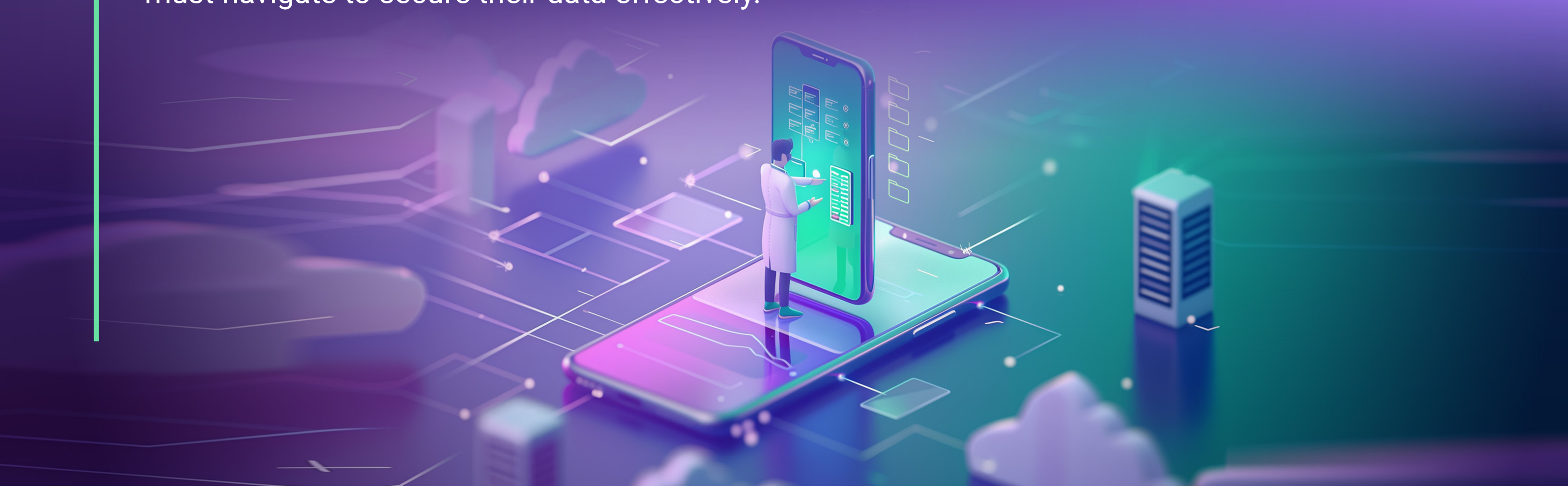
DASERA



Contents

Introduction

Data security is a lifeline in healthcare. The sensitive nature of healthcare information makes it a prime target for cybercriminals. Protecting this data is crucial for regulatory compliance, maintaining patient trust, and ensuring the integrity of healthcare services. This white paper will delve into the unique challenges and regulatory requirements that healthcare organizations must navigate to secure their data effectively.



Securing Healthcare Data Amidst Technological Advancements

Let’s dive right into it. Healthcare data is like gold to cybercriminals. Think about it: personal identification details, medical histories, insurance info, and financial records are all bundled together. This makes healthcare data a high-value target for identity theft and financial fraud. Criminals can use this information to create fake identities, commit financial fraud, and even blackmail individuals. The stakes are high, and so is the potential for misuse.

The healthcare ecosystem itself is a tangled web. We’re discussing a vast, interconnected network of providers, insurers, and technology vendors. Each player in this network handles sensitive patient information, and the data flows between them constantly. This complexity introduces significant risks, especially considering the diversity of stakeholders involved. Multiple identity issues arise because contractors and temporary staff may share IDs or have varied access levels. Keeping track of who has access to what data becomes a monumental task, and any slip-up can lead to severe breaches. In 2023 and 2024, primary healthcare providers like Change Healthcare and Ascension experienced significant breaches, underscoring that healthcare is a prime target both in the US and abroad.

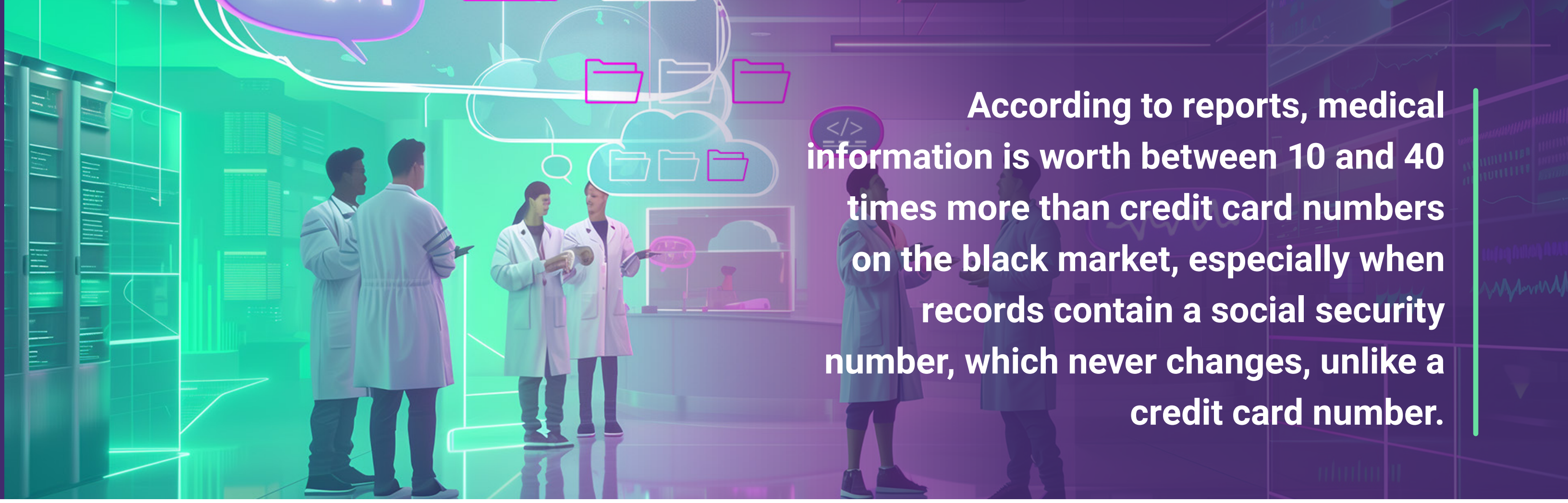
The Impact of Digital Technologies on Healthcare Data Security

In addition, the healthcare industry has transformed significantly by adopting digital technologies such as electronic health records (EHRs), remote patient monitoring, and telemedicine. These innovations have revolutionized healthcare, offering numerous benefits like improved patient care, enhanced diagnostic accuracy, and greater accessibility. However, they also introduce significant security vulnerabilities that must be addressed.

EHRs centralize vast amounts of sensitive patient information, making them prime targets for cyberattacks. While providing continuous health tracking, remote patient monitoring systems often rely on wireless communication that can be intercepted if not correctly secured. Telemedicine platforms facilitating remote consultations can be compromised through unsecure network connections, exposing patient data and communications. Addressing the security vulnerabilities inherent in these technologies is crucial to safeguarding patient data and maintaining trust in digital health solutions.

Existing patient monitoring systems, critical for continuous health tracking and chronic disease management, often harbor vulnerabilities that can be exploited by cybercriminals. Many of these systems were initially designed with low cybersecurity measures, whether due to oversight or ease of use, making them susceptible to attacks. Insecure communication channels between devices and central systems can be intercepted, allowing unauthorized access to sensitive health data. Additionally, outdated software and firmware in these devices can be exploited to gain control over the monitoring systems, potentially leading to inaccurate health data reporting or even device malfunction.

The complexity is further heightened by the vast variety of systems and devices within a single hospital room. Each piece of equipment, from infusion pumps to heart monitors, operates on different platforms and communication protocols, adding potential vulnerabilities. Integrating these various monitoring devices introduces significant challenges, increasing the risk of misconfigurations and security gaps. Ensuring the security of these systems is paramount to protecting patient information and maintaining the integrity of healthcare services.



According to reports, medical information is worth between 10 and 40 times more than credit card numbers on the black market, especially when records contain a social security number, which never changes, unlike a credit card number.

The High Value of Healthcare Data and the Need for Enhanced Security Measures

Is it a shock to anyone that cybercriminals highly covet and target healthcare data due to its comprehensive and sensitive nature? Unlike financial data, healthcare records contain a wealth of information that can be exploited for identity theft, financial fraud, and blackmail. Medical histories and personal identification details fetch high prices on the black market. According to reports, medical information is worth between 10 and 40 times more than credit card numbers on the black market, especially when records contain a social security number, which never changes, unlike a credit card number. This hijacked personal info can be used for tax fraud and other malicious activities (CyberPolicy) (HIPAA & Health Information Technology).

Healthcare organizations worldwide have faced severe breaches, highlighting the global nature of this threat. These incidents demonstrate that evolving security measures are essential. However, securing this data isn't just about fending off cyber threats; it also involves navigating a complex landscape of regulatory requirements designed to protect patient information. Understanding these regulations is crucial for any healthcare organization aiming to maintain compliance and safeguard sensitive data. Let's explore the regulatory compliance landscape in healthcare and how it plays a vital role in ensuring data security.

Regulatory Compliance in Healthcare

Healthcare organizations navigate a complex and highly regulated environment where protecting sensitive patient data is a top priority. Understanding and complying with these stringent regulations is essential to avoid severe penalties and ensure patients' trust and safety. Let's look at the key regulations crucial to healthcare data security.

Overview of Key Regulations

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA sets the standard for protecting sensitive patient information. Healthcare providers, payers, and their business associates must implement physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).
- **Health Information Technology for Economic and Clinical Health (HITECH) Act:** HITECH expands the scope of HIPAA by promoting the adoption and meaningful use of health information technology. It includes provisions to increase penalties for non-compliance and mandate breach notifications.

- **California Privacy Rights Act (CPRA):** The CPRA enhances the California Consumer Privacy Act (CCPA) by introducing stricter data privacy requirements. It grants California residents more control over their personal information, including the right to access, delete, and opt out of data sharing.
- **General Data Protection Regulation (GDPR):** GDPR is a comprehensive data protection regulation that applies to organizations handling the personal data of EU residents. It mandates robust data protection measures and grants individuals extensive rights over their data, including the right to access, rectify, and erase their information.
- **Health Information Trust Alliance Common Security Framework (HITRUST CSF):** HITRUST CSF is a certifiable framework that provides a comprehensive set of controls to manage risk and meet the regulatory requirements of various standards, including HIPAA, HITECH, and GDPR.

Specific Requirements and Penalties

Compliance with these regulations requires healthcare organizations to implement detailed safeguards and processes:

- **HIPAA and HITECH:** Organizations must conduct regular risk assessments, enforce strict access controls, provide ongoing employee training, and maintain audit trails. Non-compliance can result in fines ranging from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million.
- **CPRA:** Entities must ensure data minimization and purpose limitation and implement robust security measures. Penalties for violations can reach up to $7,500 per intentional violation.
- **GDPR:** Organizations must implement data protection by design and default, appoint a Data Protection Officer (DPO), and report breaches within 72 hours. Non-compliance can lead to fines of up to €20 million or 4% of annual global turnover, whichever is higher.

Regulatory Variations

Regulatory requirements can vary significantly based on geographic location and the type of service provided:

- **Geographic Location:** Regulations like GDPR apply broadly across the EU, while others like CPRA are specific to California. Understanding these geographic nuances is essential for maintaining compliance. An ongoing debate centers on whether EU citizens should have the same data protection rights outside the EU as they do within it. This debate can become contentious, as it involves complex legal and political considerations regarding jurisdiction and international law.
- **Service Type:** Additional regulations such as the Network and Information Systems (NIS) Directive apply to critical infrastructure providers, and the Payment Card Industry Data Security Standard (PCI DSS) applies to organizations handling payment card information. Each regulation imposes specific security controls and reporting requirements, necessitating tailored compliance strategies for different service types.

Staying on top of these regulatory requirements and implementing robust data security measures isn't just about avoiding fines—it's about protecting your patient's sensitive information and maintaining their trust. Taking a proactive approach to data security helps build confidence with patients and stakeholders, setting your organization up for long-term success.

Proactive Strategies for Healthcare Data Protection

Building a comprehensive data security and governance program is the cornerstone of protecting healthcare data. This program should clearly define the organization's scope, roles, and responsibilities, ensuring everyone understands their part in safeguarding information. Establishing guiding principles helps align the organization's security efforts with its mission and goals.

Regular risk assessments are crucial to understanding and improving the organization's security posture. These assessments help identify vulnerabilities and potential threats, allowing for timely mitigation measures. Employing robust access and identity management further strengthens security by implementing role-based access controls and minimizing the risk of unauthorized access. Ensuring that data is secure both in transit and at rest is vital; encryption techniques safeguard information during transmission and storage.

Improving security awareness and training within the organization is another essential strategy. Ongoing education programs and best practices for protecting sensitive information ensure that employees remain vigilant and informed about potential threats. This cultural shift towards prioritizing data security helps maintain high awareness and compliance across the organization.

Leveraging Data Security Posture Management (DSPM)

To enhance these proactive strategies, leveraging Dasera's advanced Data Security Posture Management (DSPM) platform can be highly effective. Dasera offers comprehensive capabilities that ensure data visibility, accessibility, and protection across a company's entire data infrastructure.

- **Automated Data Discovery:** Dasera offers automated discovery capabilities to identify all data stores across cloud environments and on-premises systems. This automation reduces manual tracking errors and ensures complete data visibility, helping organizations account for all data repositories.
- **Data Classification and Tagging:** Dasera enables accurate classification and tagging of data based on its sensitivity and regulatory requirements, facilitating appropriate protective measures and compliance with privacy regulations.
- **Continuous Policy Enforcement and Compliance Management:** Dasera continuously monitors data access and usage policies, simplifying compliance with regulations like HIPAA, HITECH, CPRA, and GDPR. Real-time policy enforcement ensures that data protection measures are consistently applied, minimizing non-compliance risk.
- **Real-Time Monitoring and Detection:** Dasera includes data-in-use monitoring to track access and use across various systems, including Electronic Health Records (EHRs) and other repositories. This helps identify potential security breaches by monitoring data flow between EHRs and other storage locations. By tracking data access and movement in real time, Dasera can detect unauthorized access or anomalies, allowing for swift responses to potential threats. This capability significantly reduces the risk of data breaches by promptly addressing unauthorized attempts to access or manipulate data.
- **Integration with Existing Security Infrastructure:** Seamless integration with existing security tools is essential for a unified approach to data protection. Dasera's advanced platform works cohesively with the current infrastructure, ensuring comprehensive coverage and simplifying data security management.

By integrating Dasera's DSPM platform with existing security infrastructure, healthcare organizations can ensure a unified approach to data protection. This seamless integration enhances the organization's ability to manage data security comprehensively, ensuring no gaps in protection.

Real-World Examples:
Omada Health's Journey to Automated Data Security and Governance

Omada Health, a virtual-first chronic care provider, specializes in preventing and treating cardiometabolic diseases, including type 2 diabetes and hypertension. Managing sensitive healthcare data on Amazon Web Services (AWS) using S3 buckets, RDS instances, and Redshift databases presents significant challenges. The scale and sensitivity of Omada Health's data make tracking data sprawl, enforcing security controls, and maintaining manual governance processes difficult.

With 250 connected data stores, including 80 in production, and 41 billion sensitive records to monitor, manual classification and tagging are impractical. Dasera has stepped in to automatically discover all data stores, classifying and tagging billions of data fields in near real-time. This capability acts as a force multiplier for Omada Health's Security team, allowing them to spend less time investigating issues and more time addressing them.

The Benefits of Dasera's Platform for Omada Health

- **Identifying Crown Jewels:** Dasera helps Omada Health identify its most valuable data by automatically tagging and classifying it based on sensitivity and regulatory requirements. This prioritization enables the security team to focus on protecting critical information.
- **Discovering Unknown Data:** Dasera has uncovered data that Omada Health may not have been fully aware of, including shadow IT copies—duplicate or rogue data stores created without formal IT approval. Identifying these assets is crucial for comprehensive data security, as they often escape regular security protocols and can become significant vulnerabilities.

- **Mitigating Data Sprawl Risks:** With data spread across numerous repositories, it's easy to lose track of its location. Dasera's real-time data discovery and tagging ensure that Omada Health maintains an up-to-date inventory of its data assets, reducing risks associated with data sprawl.
- **Enhancing Compliance Efforts:** By classifying data in near real-time, Dasera simplifies compliance with regulations such as HIPAA, HITECH, CPRA, and GDPR. This ongoing classification ensures that sensitive data is always protected and that Omada Health continuously complies with relevant data protection laws.

Enhanced Efficiency and Compliance

Omada Health aims to avoid breaches while ensuring data accessibility for patient care. As healthcare is the most breached industry in the United States, protecting sensitive health data is paramount. However, the data must remain available to care providers to improve patient outcomes. Dasera helps balance these objectives by providing robust security without obstructing data accessibility. For instance, Dasera enhances Omada Health's audit processes by identifying new data stores and generating real-time alerts when they don't match existing policies. This allows for proactive issue resolution and improved compliance.

Improved Operational Efficiency

Dasera significantly increases the efficiency of Omada Health's Security team. Previously, gathering information for cyber insurance policies took weeks, but with Dasera, this can now be done in minutes. Bill, a security leader at Omada Health, highlights that "Dasera lets me answer questions much faster, specifically about our data and our data sprawl." This rapid response capability saves time and ensures critical decisions are based on accurate, up-to-date information. By providing visibility at scale, Dasera enables the Security team to operate more efficiently and effectively, ensuring robust protection of sensitive data.

Ultimately, Dasera fills a critical visibility gap in data security and governance, allowing Omada Health to maintain stringent security standards while reducing the burden on its data engineering teams. This comprehensive approach fortifies Omada Health's security posture and optimizes its security operations' efficiency, enabling it to address potential threats swiftly and effectively.

Looking Ahead: Ensuring Future-Proof Healthcare Data Security

Throughout this white paper, we have highlighted the critical importance of data security in healthcare, emphasizing the high stakes involved due to the sensitive nature of healthcare information. We explored the unique challenges posed by the complexity of the healthcare ecosystem and the rapid adoption of digital technologies like EHRs, remote patient monitoring, and telemedicine. These advancements, while beneficial, introduce significant security vulnerabilities that healthcare organizations must address. We also discussed the stringent regulatory requirements, including HIPAA, HITECH, CPRA, GDPR, and HITRUST CSF, which mandate comprehensive data protection measures. Proactive strategies are essential, such as building robust data security and governance programs, conducting regular risk assessments, employing robust access and identity management, and improving security awareness and training. Leveraging advanced DSPM platforms like Dasera can enhance data security by providing automated data discovery, continuous policy enforcement, real-time monitoring, and seamless integration with existing security infrastructure.

Future Trends in Healthcare Data Security

Looking ahead, emerging technologies will continue to shape the landscape of healthcare data security. Innovations like artificial intelligence (AI) and blockchain can dramatically evolve data protection. AI can enhance threat detection and response capabilities by identifying patterns and anomalies in real time, while blockchain offers a decentralized and tamper-proof method for securing health records. However, these technologies also bring new challenges and vulnerabilities that must be addressed proactively.

Anticipated regulatory changes will also significantly impact healthcare data security. As data privacy concerns grow, regulations will become more stringent, requiring organizations to adopt more rigorous data protection measures. Staying abreast of these changes and adapting quickly will be crucial for maintaining compliance and safeguarding patient data.

Expanding Beyond Healthcare: Implications for Other Regulated Industries

While this white paper focuses on the healthcare sector, the principles and strategies discussed are equally relevant to other highly regulated industries, such as finance, legal, and government. These industries also handle sensitive data and face similar challenges regarding data security and regulatory compliance. Leveraging advanced DSPM platforms like Dasera can provide comprehensive data protection, ensuring compliance and building trust with stakeholders across various sectors.

Now is the time to act! The importance of staying compliant and protecting patient data cannot be overstated. By embracing these proactive measures, healthcare organizations can confidently navigate the complexities of the digital age, safeguarding the invaluable data entrusted to them. Contact Dasera today to learn how our advanced data security solutions can help you enhance your data protection, ensure compliance, and build trust with your patients and stakeholders.

REQUEST A DEMO

DASERA