Practical Guide for the Healthcare Sector

How to safeguard patient data within a modern digital healthcare infrastructure.

Whitepaper

Introduction

As digital technology becomes increasingly central to our lives, so the critical services we depend on also need to be managed digitally. In the healthcare sector, this transformation manifests itself in the digitization of diagnoses and treatment recommendations, prescriptions, and other patient-specific data. Controlling this extremely sensitive and potentially life-changing information demands that protecting digital data and devices against theft, loss or misuse becomes mission critical for all healthcare organizations.

The essential nature of data protection within the healthcare industry is not only being driven by increasing volumes of sensitive digital patient data. Patient data security and privacy regulations are also increasing in number and complexity in the digital era. In the US, these include Personal Health Information Protection Act (PHIPA) or the Health Insurance Profitability and Accountability Act (HIPPA) among many others. In Europe they include the EU's General Data Protection Regulation and numerous other country- and industry-specific statutes. Failure to abide by these regulations can expose healthcare organizations to very significant financial penalties and legal expenses, sometimes measured in the millions of dollars.

At the same time, the number and severity of data security breaches caused by externally driven cyber-attacks using malware, ransomware or data exfiltration is significant and growing. For example, in the US, the HIPPA Journal reported a 25% increase in breaches between 2019 and 2020. Not only that, according to the Carnegie Mellon University Software Engineering Institute, more than half of insider fraud incidents within the healthcare sector involve the theft of patient data. The financial and reputational risks associated with these external and internal attacks are also significant.

Add the potential for “honest” process failures and mistakes into the mix, and it's clear that protecting patient data effectively has never been more difficult yet essential than it is today.

25%

increase in breaches
in the USA between
2019 and 2020

Healthcare organizations are underprepared

In this context it is pretty concerning that many healthcare organizations are not well equipped to deal with this rising tide of threats to data integrity. There are a number of reasons for this:

- **Infrastructure and data source complexity:**
  Patient data exists in multiple formats and on multiple systems. This makes it challenging to manage data protection in a holistic way.

- **Insufficient data encryption:**
  When patient data is stored within access-restricted internal systems, it is often deemed "secure enough" that data does not need to be encrypted. As numerous successful hacking attacks and incidences of internal data theft or misuse have proven, this is not the case.

- **Attack surface opacity:**
  Without centralized and comprehensive IT asset management, it is impossible to establish a clear, accurate picture of an organization's potential attack surface. Even with IT asset or device management in place, medical machines and employee's personal devices are often excluded from that management environment.

- **Lack of data traffic visibility:**
  IT asset management that omits the capability to track network data traffic in real time cannot be truly effective, because anomalies become much harder to identify.

- **System access restrictions:**
  Without the appropriate management solutions in place, restricted access to some systems further reduces the visibility of certain data and devices.

- **Poor policy standardization:**
  When data transfer security is handled in multiple ways depending on the system and situation, the risk of mistakes being made, or security vulnerabilities being created increases significantly.

- **Resource-restricted IT teams:**
  In addition to general IT understaffing, data protection specialists are scarce and dedicated Security Operations Centers are prohibitively expensive for many healthcare organizations.

- **Little or no security management automation: :**
  Given the scarcity and expense of dedicated data protection resources, automating data protection processes is essential. But the healthcare sector as a whole has little automation in place, especially when it comes to integrating data protection into IT Service Management and device management systems.

3 Steps to Complete Patient Data Security

It’s clear that many healthcare organizations urgently need to ramp up their data protection capabilities. But it’s equally clear that to be truly effective, data protection should be part of a holistic, integrated approach to data, device and IT service management. It should also be highly automated, easy for a small team to control and cost-effective.

Ultimately, an optimal approach needs to ensure three things:

1

Visibility:

To protect data comprehensively, you need a complete picture of what data you have, where it resides, who is using it, and how it’s moving around within networks and between devices.

2

Insight:

Once you establish visibility over data and devices, you need an auditing infrastructure to ensure you understand what you have, how it is changing, and when it needs to be updated, retired or replaced.

3

Protection:

Finally, data protection requires effective access control, data encryption and policy setting, as well as seamless integration with your IT service management and unified endpoint management infrastructures.

An integrated, single-source management solution that achieves all three of these objectives is the most effort- and cost-effective way to achieve holistic data protection. Specifically, it should enable single console management of device and access control, data encryption, data flow monitoring and user behavior analytics, as well as offering post-infection protection against malware-instigated data exfiltration.

The benefits of deploying such a solution include faster IT rollouts, simpler administration, and reduced risk thanks to real-time automated security updates, threat detection and data defense measures.

The solution you select should offer as many of these features as possible to ensure a holistic, integrated and robust approach to patient data protection.

Your Patient Data Protection Solution Checklist

- ☑ Unified endpoint management featuring automated software allocation with integrated whitelisting.
- ☑ Proactive data protection through secure device lifecycle management from initial installation to final decommissioning.
- ☑ Secure onboarding of employees to ensure safe, productive working from day one.
- ☑ Effective extension of data protection for remote workers and devices.
- ☑ Improved cyber-resilience through automated defense against malware and recovery at the endpoint.
- ☑ Enhanced transparency with data vulnerability analysis at the touch of a button.
- ☑ Automatic, analysis-based anomaly detection and elimination of insider attacks.

Deploying a solution with all these attributes to manage your valuable patient data will help you:

- **Maximize your IT budget** by consolidating client management, mobile device management and security management within a single solution.
- **Respond more quickly and effectively to cyber-attacks** with an automated system to deal with everything from threat detection to recovery.
- **Higher cyber-resilience and productivity** through standardized process for always protecting data, within onsite networks and when being accessed by legitimate external users.
- **Efficient use of scarce IT resources** through easy administration within a single management console.
- **Faster, easier compliance** thanks to native security integration.
- **Peace of mind** through at-a-glance access to security status and vulnerability analyses that generate alerts about potentially suspicious behavior.

Matrix42 offers the most comprehensive data and device management solution to achieving all of this and more for your healthcare organization.

Locations

Headquarters Germany
Matrix42 AG
Elbinger Straße 7
60487 Frankfurt am Main
Germany
Phone: +49-69 6677-38220
Fax: +49-69 6677-88657
info@matrix42.com

Branch office for the Americas
FireScope, Inc. - a Matrix42 company
412 Olive Ave, Suite 603
Huntington Beach, CA 92648
USA
Phone: +1 657-204-0993
sales@firescope.com

Further offices abroad
can be found on our website:
www.matrix42.com

About Matrix42

Matrix42 helps organizations digitize and secure the workspace environment of their employees. The software for digital workspace experience manages devices, applications, processes and services simple, secure and compliant. The innovative software supports the integration of physical, virtual, mobile and cloud-based workspace environments seamlessly into existing infrastructures.

Matrix42 AG is headquartered in Frankfurt am Main, Germany, and distributes and implements software solutions with regional and global partners.