5 Tips to Help Protect Your Data

Healthcare: From passive monitoring to proactive protection
# Table of Contents

**Healthcare Providers Face Critical Data Protection Challenges** ........................................... 3  
1. Identify a Data Protection Champion in the Organization, but not in IT ........................................... 4  
2. Build a Governance Team with Distinct Roles ................................................................................. 4  
3. Start with Policy, Awareness, Compliance, and Remediation .......................................................... 5  
4. Get to Action, Not Just Monitoring ...................................................................................................... 5  
5. Build Rules That Are Both Content- and Context-Aware .................................................................... 5  
**Key Takeaways** ........................................................................................................................................ 6  
**Intel Security Data Protection Portfolio** .................................................................................................. 6
Last year we published a report on data exfiltration, which found, among other things, that about 20% of data losses were attributed to accidental actions by internals; another 20% to intentional actions by internals; and the remaining 60% by external attackers. With the numbers of attacks and breaches growing each year, cyber attacks are fast becoming an ongoing fact of modern life.

For healthcare providers, the problem is heightened. Stolen data is most commonly critical information such as medical records and other personal data, and the risks are increasing with the growth of electronic medical records systems, electronic patient-doctor communications, and Internet of Things (IoT) devices that enable remote patient support. And all of it occurs under the specter of robust HIPAA compliance and security regulations.

Risks are everywhere, and the key is to manage them. So the next step is to move from passive monitoring to more protective blocking of sensitive and confidential data. The trick is to do this with the smallest number of false positives and minimal impact to legitimate organizational processes. Towards that, we have identified five tips, based on real-world deployments and experience, which will enhance your data loss prevention (DLP) implementation.

**Healthcare Providers Face Critical Data Protection Challenges**

As healthcare providers expand use of EHR systems, including patient access alternatives, the data environment becomes more challenging to protect. And the internal data sprawl is spreading across connected medical devices and remote IoT devices that open more susceptibility to both accidental data loss and intentional data theft. Existing organizational processes and security training simply cannot keep up, and require a different approach.

Yet the advantages of equipping healthcare practitioners and facilities with advanced technology solutions must be viewed in light of risks of security breaches, potential network vulnerabilities, and compliance issues. According to the Ponemon Institute’s fifth annual benchmark study on patient privacy and data security, more than 90% of healthcare organizations experienced a data breach in the past two years, and 40% experienced more than five data breaches within the same time period.

The high black-market value of healthcare data and personally identifiable information (PII) has led to attackers targeting vulnerable healthcare infrastructures, including ubiquitous mobile devices. Patients are also more educated and adamant about asserting their privacy rights, even as they demand more convenient access via mobile apps, wearable devices, and patient portals.

Under pressure from regulators and the public, healthcare IT teams are looking to react faster to detect and mitigate risks, and identify where to implement next-generation controls to ease the security and compliance burden. As the healthcare industry becomes more competitive, IT teams are also expected to enable new patient-facing services, from Wi-Fi throughout the hospital environment to advanced digital medical systems.
Existing organizational processes and security training cannot keep up, requiring a different approach. A modern DLP process needs to be rapidly incremental, focusing on derived value, successful preventative actions, and increasing the risk threshold. Data protection is a job for the whole organization in order to successfully prevent data loss. This requires:

1. A data protection champion who is not in IT
2. A governance team
3. An appropriate starting point
4. A bias towards blocking
5. Rules that are context-aware

1. **Identify a Data Protection Champion in the Organization, but not in IT**

Data loss prevention is a continual journey, one that requires the efforts of the entire healthcare organization to be successful. This cannot be treated as a purely technical issue, with data protection run solely by IT. IT may be responsible for the specs, implementation, and operation, but they cannot be held accountable for the actions and behavior of the whole organization and all its individuals. The majority of breaches involve at least one human vulnerability or exploitation, whether that is a phishing email, credential theft, or malware infection. It is important to treat this as an organizational problem, so it requires a data protection champion that is part of the organization.

Too often, healthcare facilities, units and departments do not operate at a continuously high level of security awareness. Security training, process changes, and news about other data breaches may briefly heighten awareness, but that can quickly fade. A champion from the organization can communicate the imperatives of protecting networks and data, lead other unit and department managers to be champions within their own areas, and better identify conflicts between DLP best practices and essential organizational processes.

2. **Build a Governance Team with Distinct Roles**

The data protection champion, while highly visible, is one part of a broader data governance team, which is a DLP best practice. It takes a diverse group, representing multiple aspects of the organization, to make this work effectively. Security by decree is prone to resistance and too many exceptions.

Effective governance teams include four distinct roles:

- One role is those responsible for defining and implementing security solutions and practices, such as the CIO, CISO, and privacy or risk officers, depending on the structure of the organization. This group is there to provide expertise on available technology, best practices from other healthcare organizations, threat updates, and continual feedback on what is and is not working.

- Next are the individuals who are ultimately accountable for the success or failure of the security operations -- the CEO or departmental leaders, as well as the owners and creators of the data. The data owners and creators are essential to designing secure processes that do not hinder key processes such as providing care to patients, yet have few, if any, exceptions.

- Consultants on legal, regulatory, and other external factors are another important part of the governance team to ensure that processes and technologies work in concert with HIPAA as well as other legal and privacy considerations. This part could include legal counsel and privacy advocates, as well as human resources professionals.

- Finally, the governance team must include representatives of those who will be working daily with the security processes, so they are part of the discussion and can inform both the governance team and their peers of the issues. Their inclusion helps ensure that relationships are not compromised by security practices.

Data governance is an ongoing activity that cannot do everything all at once. Start by designing a plan that provides overarching guidance, then implement it, expand it, and continue to adapt to the evolving nature of security, privacy, and data.
3. Start with Policy, Awareness, Compliance, and Remediation
The purpose of the data governance team is planning and implementing DLP processes. However, it should be immediately recognized that this is a continual journey, not a destination. Data is constantly growing and moving, with new types and classifications appearing, and policies and regulations evolving. It is important not to get stuck on any one area, whether it is policy, compliance, or discovery.

Many healthcare providers start the process with discovering and classifying their data, but this itself can be an endless task. It is far more important to start by discovering what is leaking out (or being stolen), and at the core of this are the security policies. Policies can be developed quickly and refined over time, if they focus on the principles instead of the particulars. For example, a policy could be that all data in transit needs to be encrypted, not the details of the technology and processes that make that happen.

Armed with a set of policies, communication and awareness is the next key step. DLP means blocking activity, since any incident that is not blocked is a breach. Communicating it effectively will make dealing with false positives much easier. A false positive can be annoying, frustrating, and slow down organizational processes, but does no long-term harm. A false negative is a breach. The focus should be on quick wins for better compliance and faster remediation, not a global understanding of all your data while leaks continue.

4. Get to Action, Not Just Monitoring
If you assume you are already leaking data, the goal is to get to action as soon as possible, addressing the big risks first. Simply monitoring data losses adds no value to the organization, and could immediately compromise patient privacy. The easiest progression is from data at rest, to data in motion, to data in use, but that should be modified by your knowledge of what is happening in the organization.

Initial deployments should target false positives between 5% and 10%, which are then quickly analyzed to improve blocking efficiency. If your false positives are too high (and they can approach 30% in typical drop-in deployments) the end result is workarounds and a return to monitoring only. Instead, build gradually, targeting the biggest risks and leakages. There is a direct but inverse relationship between false negatives and false positives -- increasing the sensitivity decreases false negatives but potentially increases false positives. Increasing the sensitivity of the risk threshold as the rules are refined to be optimally effective will improve your loss prevention successes, while keeping false positives within a manageable range.

5. Build Rules That Are Both Content- and Context-Aware
The hard work in all of this is defining and refining the rules that implement the policies and ultimately block potential data loss. The challenge here is to reduce the number of false positives while increasing the risk threshold, which is accomplished by adding context, sensitivity, and specificity to your rules.

For example, an obvious rule is to block documents that include social security numbers (or their equivalent), which in the United States is a nine-digit number of the form 123-45-6789. This seems straightforward, using the pattern-matching capabilities of regular expressions. However, a nine-digit number could also be a mobile phone number in Singapore, a Twitter handle, a US Zip+4 code, or a PDF document number. So, to reduce the false positives, you need more context for the usage of the data or document, the severity of the potential loss, and the likely sensitivity of it.

For example, you can count to see how many instances of a similar type of data are found, and set an initial severity threshold. You can look at how close they are to other personally identifying information, such as a date of birth or credit card number. You can search for textual identifiers close to the risky data, such as “SSN,” “First Name,” and “Last Name.” Compounding these factors together can reduce the numbers of false positives by 50% to 70%.
To aid in this activity, the governance team must clearly communicate that they are implementing the DLP plan, and that people who run into blocked data should call the help desk. Analyzing these notices, which could be either a viable process or a true positive, will give you additional factors for the rules and improve efficiency. It is important that more than one person is involved in creating rules, investigating incidents, and dealing with those responsible, so there is a separation between police, judge, and jury. Block the worst first, and continue iterating until you reach the desired risk threshold.

**Key Takeaways**

The costs of data breaches in healthcare (both dollar and human) have increased significantly over the past several years. Whether you are trying to stop data breaches, demonstrate regulatory compliance, or gain visibility and control of your data across different devices and clouds, an integrated and collaborative approach is necessary.

Implementing these five tips will help your organization establish a comprehensive data protection program and better manage the risks of data loss and theft. The benefits of this type of program extend beyond preventing data leakage to include earlier detection and mitigation, reduced time and cost of breach investigations, enhanced compliance and reporting, and increased comfort level of senior management with the organization’s risk threshold.

**Intel Security Data Protection Portfolio**

The Intel Security suite of integrated security solutions helps ease the burden and cost of healthcare security and risk management, providing faster protection from emerging threats, stronger security policy management, and more robust security for medical devices. Healthcare risk management is not just about managing HIPAA or regional compliance, but creating faster medical data breach detection with our Security Connected framework, which protects the privacy of patients. Security management that encompasses mobile devices and systems, with supporting network, application, and data security, provides essential protection for healthcare services. And our continued effort working with manufacturers and healthcare providers is driving better medical device security.

From endpoint encryption to DLP technology, and from centralized common policy management to automated reporting, Intel Security works closely with an extensive community of technology and business partners to deliver the customization and flexibility your healthcare organization needs. Whatever stage you are at in your data protection process, Intel Security solutions and professional services can help you define metrics, offer guidance on best practices, and ease your deployment.

To learn more about our data protection products, please visit:

www.mcafee.com/healthcare

www.mcafee.com/dataprotection

To learn about designing and evaluating a data protection program, please visit:

www.foundstone.com
Work smarter.

At Insight, we’ll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more