CGI

Experience the commitment®

Cyberprivacy and Cybersecurity for Health Data

Building confidence in health systems

Providing better health care quality at lower cost will be the key aim of all health economies over the next 20 years, and data analytics will play a powerful role. Its greatest impact will be less retrospective (what happened), and more predictive (what might happen) and prescriptive (what could happen). Combined with precision medicine based on molecular profiling, data analytics will help drive change that benefits all who receive, deliver, and pay for healthcare.

Given that health data provides such a vital resource, but also contains some of the most sensitive information available, this paper offers key considerations for improving privacy and security postures in a continuously evolving landscape. This is the first in our viewpoint series on “Data and the Future of Healthcare,” and will be followed by papers on secondary uses for health data, and innovative ways of using predictive analytics to achieve needed transformation in healthcare.

Introduction

In recent years, healthcare providers, payers and regulators have been subjected to ever-increasing data privacy concerns and security risks affecting their operating and legislative environments as well as patient confidence. Cyber-attacks are on the rise as health organizations strive to use more electronic services to increase connectivity for workers and patients. Personal health and lifestyle information is increasingly valued as a commodity by cyber-attackers.

From personal medical devices to enterprise-wide platforms, systems are being targeted maliciously with resulting data losses. Onerous compliance requirements are exacerbated by the scarcity and high cost of skilled privacy and security resources, complex and risky IT technology, and increasingly dangerous and pervasive cyber threats. As healthcare moves increasingly outside hospital walls and into homes and communities using consumer-based technologies, patient trust in providers must extend to the data and new devices used for monitoring and treatment. Health organizations must weigh carefully how to address their privacy and security needs in a cost effective manner.

Data privacy and security challenges in healthcare

Too often, healthcare organizations do not understand their information privacy and security risks, or know where to start to improve their security posture. Similarly, with the spread of federated system access to data, many organizations are not compliant with evolving legislation intended to protect the privacy of personal information. Delivering better health outcomes at a lower cost while remaining compliant requires a comprehensive understanding of the risks involved in dealing with health consumers, staying connected to them, and ensuring their sensitive information is kept private and secure.

As reported by Reuters, the U.S. Federal Bureau of Investigation has warned healthcare providers that, "The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."[1]

Most providers lack the capacity or financial means to effectively address their growing challenges in areas such as:

- Compliance with privacy, consent and other regulatory requirements
- Identity and data loss theft
- Shortage of skilled security professionals
- Consumerization of healthcare or Bring Your Own Device (BYOD)
- Assessing their safeguard effectiveness
- Improving and maintaining employee privacy and security awareness.

Cyberprivacy and cybersecurity are more than policies, security guards and audits. They are about having a foundation to support existing and future business growth in a manner that is compliant, cost effective and secure. Without a solid privacy and security framework, health organizations will operate with an increasing amount of risk as they strive to deal with ever growing threats and evolving legislation.

Without a solid privacy and security framework, health organizations will operate with an increasing amount of risk as they strive to deal with ever-increasing threats and evolving legislation.

[1]Exclusive: FBI warns health sector vulnerable to cyber attacks, Reuters, Jim Finkle, April 23, 2014

Adapting privacy and security programs to new business models

Ensuring compliance with increasingly complex data privacy, access and audit legislative requirements creates challenges in preventing unwarranted access by both authorized and unauthorized users alike.

The healthcare industry is faced with a unique set of business, environmental and technical drivers of risk, along with a unique set of regulations for personal information and health data management.

Healthcare IT departments, focusing on the clinical transformation agenda, often treat patient privacy as policy, and only perform IT security as a secondary function. The scarcity of skilled information privacy and security professionals also creates risks. Security programs often lack adequate policies and procedures, and do not have modern, effectively integrated security technology.

Additionally, privacy programs often have no ability to govern access, or to audit access to data across the full extent of the systems that propagate Personally Identifiable Information (PII) and Patient Health Information (PHI). For example, in many institutions, it is common practice for health systems to share copies of production data with their suppliers who are tasked with maintaining software and resolving defects that appear in production systems.

Healthcare providers, particularly hospitals and clinics, are highly dependent upon wireless networks and mobile technology to transmit sensitive PHI to end-user devices that are poorly secured. Such systems and mobile applications are vulnerable to hacking, monitoring and data compromise, creating both liabilities and non-compliance issues that can result in legal prosecution.

Healthcare organizations also now share PII and linked datasets in health information exchanges, research networks, insurance networks and public portal internet access points and supplier networks. Ensuring compliance with increasingly complex privacy, access and audit legislative requirements creates challenges in preventing unwarranted access by both authorized and unauthorized users alike.

- U.S. healthcare providers are subject to the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) which stringently enforces protection of PHI data.
- Canada's Personal Information Protection and Electronic Documents Action (PIPEDA) regulation provides similar privacy enforcement.
- Across the European Union, a variety of federal and member state directives provide similar guidance and restrictions for the transmittal of personal health data.

Many healthcare organizations also must process and store sensitive credit card data, making them subject to the demanding, strictly enforced and audited Payment Card Industry Digital Security Standards (PCI DSS). For these healthcare organizations, PCI DSS compliance requires that security controls be sufficient for the credit card industry and systems using the credit card data. But, what about the security of the rest of the organization? Putting in place an insufficient program can result in major breaches, reputational damage, and even business failure.

In the U.S., healthcare also has been identified as one of 16 critical infrastructure sectors by the Department of Homeland Security and is subject to Presidential Executive Order 13636 and the accompanying "Framework for Improving Critical Infrastructure Cybersecurity" issued by the National Institute of Standards and Technology (NIST). While the new cybersecurity framework is voluntary, the U.S. Privacy Act and its many legislated enhancements over the last four decades are not. For this reason, there is increasing pressure for critical infrastructure organizations to adhere to U.S. privacy law and to adopt the cybersecurity framework which supports this law. Courts and insurance companies are now using it as a measure for best practices and determining risk and liability.

Comparing cyberprivacy and cybersecurity frameworks

Because there often are misconceptions about key elements of cyberprivacy and cybersecurity, it is important to have a common understanding. The following table compares the five key elements of privacy and security frameworks and demonstrates how they are aligned.

Key Framework Elements

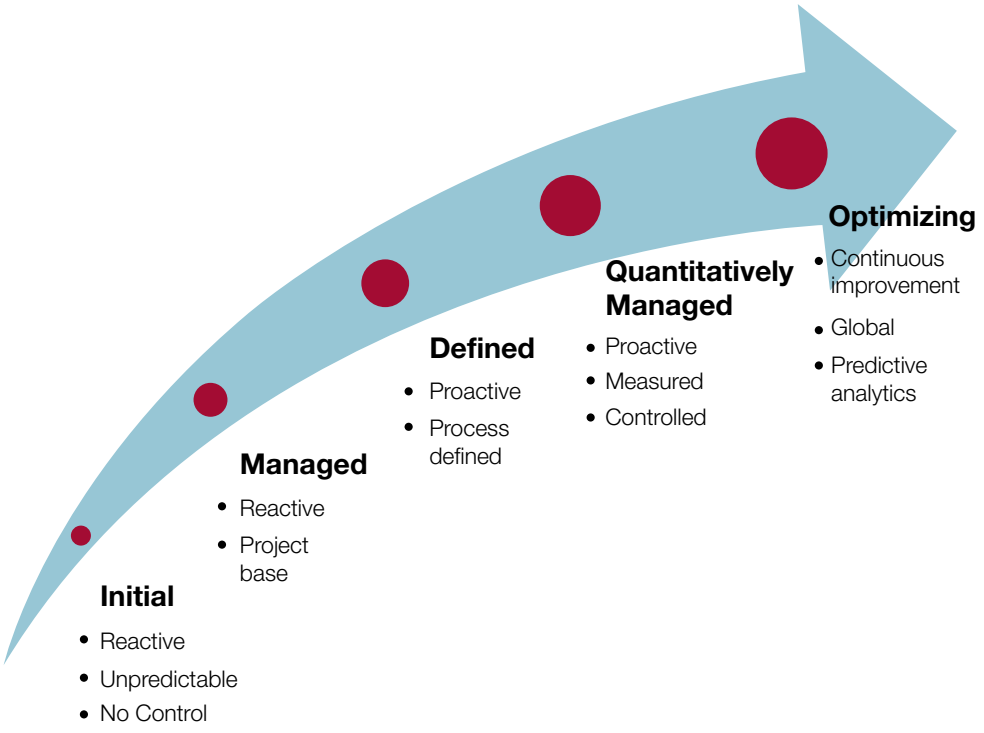
Cyberprivacy	Cybersecurity
Minimize Data: Only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).	**Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Limit Use: Use PII solely for the purpose(s) specified in the notice to the identified person by the collecting organization. Sharing PII with an outside organization should be for a purpose compatible with the purpose for which the PII was collected.	**Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Data Quality and Integrity: Ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.	**Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Secure: Protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure	**Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Audit and Accountability: Audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.	**Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Improving privacy and security confidence

While privacy and security risk can be managed, it cannot be eliminated. Yet, healthcare organizations need to have confidence that their risks are being managed to enable secure, compliant operations on an ongoing basis. Customers depend on healthcare services and trust that their information will be kept private and secure. They also need the confidence that healthcare providers have the governance and supporting infrastructure in place to adhere to a growing number of industry requirements.

This confidence can only be established by understanding the provider's complete risk posture, and implementing a program to address those risks with appropriate controls, provided in a systematic manner and based on a continuous risk improvement lifecycle.

Continuous Risk Improvement Lifecycle



Privacy and security are not piecemeal or one-time things. They must be addressed in a lifecycle approach that involves the management, technical and physical aspects of the organization. The organization and its federated partners must be assessed from end to end to identify areas that are lacking, and address those gaps with appropriate strategy and controls.

The value of privacy and security as a service

The increasing complexity of tracking where and why data is made available, and who has or had access to that data, makes it even more difficult to comply with privacy and security requirements. Some healthcare organizations are considering managed privacy and security services (MPASS) in which experienced business partners take responsibility for assessing privacy impacts and security postures, and reducing risk-related vulnerabilities and non-compliance. This allows healthcare organizations to focus more on platforms, policies and their core business.

Those who have pursued this strategy are experiencing a wealth of advantages by leaving the technology and services associated with privacy and security in the hands of experts. In addition to strengthening their privacy compliance and security postures, they are reducing their costs and risk.

MPASS partners assume some liability for threat risks as well as the responsibility for implementing a privacy and security governance framework and enabling privacy, security and audit solutions. It is important to consider the risks associated with operating in a larger network of healthcare providers when evaluating the business case for in-house versus MPASS models. MPASS arrangements can make significant contributions to regulatory compliance, and assist in-house privacy and security teams when the additional complexities of operating within different networks of partners are taken into account.

Conclusion

The challenges of protecting health data are nearly as vast as the many uses they suggest. Privacy and security frameworks must be well understood, and programs must be adapted to new business models to achieve greater confidence. Health organizations must weigh carefully how to address their privacy and security needs in a cost effective manner. This requires an understanding of their complete risk posture and implementing programs to address those risks. The increasing complexity of these challenges has led some healthcare organizations to consider managed privacy and security services to strengthen their postures and reduce their risks.

Why CGI?

CGI brings proven expertise, tools, methodologies and services for improving healthcare organizations' privacy and security confidence while meeting customer and regulatory requirements. Our privacy and security team members have gained extensive knowledge through security work within health, as well as retail, hospitality, financial services and other industries. Using a combination of this knowledge and technology-based methodologies, we establish an overall risk management framework that takes into account each client's unique risk profile and regulatory and privacy requirements.

Privacy and security are part of everything we do. We assist healthcare organizations with establishing more confident and effective privacy and security programs by identifying and addressing vulnerabilities across the healthcare enterprise. Examples include privacy assurance and secure EMRs for millions of citizens, including UK military members, and support of interoperable EMRs and registry and data warehouse solutions. Our work with clients across the globe also gives us a 360 degree view of global and local threats in both the public and private sectors. CGI's end-to-end cyberprivacy and cybersecurity offerings for health include:

- **Enterprise privacy and security management—** articulating governance and policies to help clients make smarter investments, and identify the costs, benefits, risks and opportunities associated with deploying new strategies, and leveraging existing security investments.
- **Privacy and security architecting and engineering—** designing, developing and deploying effective cyber-privacy and cybersecurity solutions.
- **Privacy and security as a service—** leveraging expert staff and advanced technologies to achieve the highest levels of privacy and security and regulatory compliance for our clients, while reducing their costs by 20%-40%. These services are delivered through 10 Security Operations Centers that continuously identify and monitor cyber threats.

cgi.com

Founded in 1976, CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and managed services. With 68,000 professionals in 40 countries, CGI has an industry-leading track record of delivering 95% of projects on-time and within budget, aligning our teams with clients' business strategies to achieve top-to-bottom line results.