CGI

Experience the commitment®

WHITE PAPER

U.S. Healthcare Data Security

The Problem with the Future is the Past

For more than a decade, U.S. healthcare and related enterprises have struggled to comply with the data privacy requirements of government regulations—not entirely for technical reasons, but also because the healthcare industry historically and culturally has been a user of technology that stands apart from business governance. Because regulatory requirements exceed traditional data center and technology boundaries, and because more privacy legislation is inevitable into the future, a response is needed by the entire healthcare enterprise, from the executive suite to patient services.

THE HEALTHCARE EXECUTIVE CYBERSECURITY DILEMMA

Numerous articles have been written concerning the executive dilemma of data security and particularly data privacy in the healthcare and medical solutions industry. As an example, the *Wall Street Journal* reported on a survey of 1,034 directors by the National Association of Corporate Directors which found, "Directors on corporate boards continue to struggle to understand cybersecurity risks," and that, "A subset of the survey shows that health-care directors admit to the least understanding, with 30% saying they have 'little knowledge' about such risks."[1]

A subset of a National Association of Corporate Directors survey shows that health-care directors admit to the least understanding, with 30% saying they have 'little knowledge' about such risks.

Much recent executive attention to health cybersecurity has percolated to the front page because of the massive Affordable Care Act healthcare insurance initiative in the United States. There also has been concern raised around the interconnectivity being built into consumer products and medical devices, also referred to as "The Internet of Things." Hackers getting access to a personal bank account is bad enough, but the potential to hack into things like an automobile, electric meter and electronic medical devices or records is overwhelming.

All elevated attention aside, the core issues are not new, and the solutions that can help effectively manage cybersecurity risks are based on long-standing policies, procedures and techniques. Healthcare and related service industries may have touched on many of these core issues for many years, and perhaps that is the root cause for the current gap in healthcare executives' understanding of cybersecurity risks.

HISTORICAL HEALTHCARE DATA PROTECTION

This is because most healthcare systems have collected and stored patient data, medical diagnoses data and post-diagnosis activities for a long time. Legacy applications developed even decades ago continue to provide mission-critical functions today. Medical payer services also have borne a substantial share of the operational processes for years. Such business functions are difficult and slow to change to support a compliant, "regulation-rich" profile.

In addition, at the executive level in healthcare, CxO's and Boards sometimes view cybersecurity as a technical obstacle, and not a business obstacle, which involves some re-education. The challenge is to address both data protection and regulatory reporting, often to satisfy several masters.

THE NEW IMPERATIVES OF HEALTH DATA SECURITY

A number of key considerations must be addressed when seeking to protect health data.

The first is to group the security needs by addressing data attributes to make it easier to offer credible and auditable security. Three grouping attributes that are among the most important to address are privacy, lineage and disposition:

- **Privacy,** along with the overarching concept of consent, is very important. In many countries, consumers provide consent for professionals to document their care electronically. Increasingly, our data needs to be shared with other professionals and agencies outside the facility where consent was granted.
- **Lineage** allows care providers to determine the initial source of the data, and what happened to it through its various locations and transformations. Sometimes, we make the presumption that consent is transportable, and there are mechanisms to document this attribute, but we need to articulate this need when the data is first defined or applied within a business application.

[1] Wall Street Journal; July 1, 2015; "Boards Struggle With Cybersecurity, Especially in Health Care"; Kim S. Nash

- **Disposition** is like an inverse of lineage in that it defines how the data is destroyed, archived and rendered unusable. In its full implementation, disposition is transferred to all instances of the data item. If a recorded symptom, diagnosis, payment, or any other protected data item is declared obsolete or invalid, that condition should be reflected in all locations where that data item is present. Multiple locations of controlled data presents a challenge much in the same way a forwarded e-mail or social media comment does. When replicated, it becomes a difficult control obstacle.

A second important consideration for healthcare data security is protecting the identity of people who have contributed their medical status or treatment results to a learning repository that improves medical treatment. For research purposes, we need to anonymize data. However, as queries narrow a solution data set to a small or even a single sample, we risk breaching privacy rights. It's a difficult task to make sure that small-cell anonymization is not compromised.

A third consideration is the ability of the healthcare industry to use medical devices that contain embedded technology, especially technology that has an interconnectivity function. It is fundamental to secure the healthcare network, but this also means managing the multitude of devices in our healthcare environments. This is no easy task, as everything from blood pressure monitors to MRIs can contain IP addresses. This is a challenge especially for devices that are critical to patient lives, such as Implantable Cardioverter Defibrillators (ICDs), pacemakers, invitro insulin pumps, etc. Devices that are not included in the typical IT security review process pose a major challenge to many leading providers. The security review of these components must be conducted by the medical community, and not just entrusted to the device provider. Accountability cannot be delegated for this critical operational element.

These challenges do not fit into the current security environment of most contemporary healthcare enterprises. The past practices of using cost-effective outsourcing providers for "sensitive" issues like patient billing and disease research have allowed healthcare providers to concentrate mainly on patient treatment, which is a good focus, but has allowed the evolving concerns around privacy and security to be unaddressed.

The healthcare provider today is being called to account, and that means the need to understand the issues and processes used to manage the evolving security challenges. Clarifications and amplifications of the role of technology, security, privacy, and/or THE compliance officer are warranted and demanded by this changing landscape. Boundaries are being erased and responsibilities expanded for healthcare organizations that are aligned with public and legislative expectations.

PRESCRIPTION FOR IMPROVED PROTECTION

The healthcare data security prescription that CGI suggests is a combination of three things:

1. **An inventory** of "protected" data items, their attributes and the applications that create and use them
2. **A business-oriented risk assessment** of what the loss of confidentiality, integrity or availability means to the enterprise in objective (money) and subjective (reputation) terms
3. **An iterative action plan** to create an environment of "improving" data security in the System Development Life Cycle, ongoing data center operations and a general employee and partner focus on good security hygiene.

Good security hygiene is at the core of the regulatory obligations embodied by the U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) regulations and other privacy regulations. In this context, hygiene means the regular, reliable management of sensitive, protected data and its attributes so that, on any given day, the usual and customary practice followed by all staff members and business associates is appropriate, documented and reportable.

Paraphrasing a toothpaste commercial from the 1960's, a healthcare enterprise's treatment of data security could be "shown to be an effective preventative that can be of significant value when used in in a conscientiously applied program of good practices and regular professional care."

CONCLUSION

Healthcare enterprises must break the mold of the past to strengthen their security postures and comply with data privacy requirements. Historical approaches must make way for a new kind of thinking. What is needed to begin this journey is an inventory of protected data, along with the lineage of where the data originated and to whom it has been forwarded. It is also critical to remember that this is an ongoing process, because application systems and business environments change. The best strategy is one of continuous improvement—not a project with a finite completion date. CGI's white paper on "Cybersecurity for Health Data: Building confidence in health systems" discusses additional considerations for improving healthcare data privacy and security postures in a continuously evolving landscape.

For those enterprises that fail to start this process while waiting for the business to "stabilize," chances are it probably won't, so start anyway. What are we waiting for?"

WHY CGI?

CGI brings proven expertise, tools, methodologies and services for improving healthcare enterprises' privacy and security confidence while meeting customer and regulatory requirements. Our privacy and security team members have gained extensive knowledge through security work within healthcare, 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.

cgi.com/health