OVERVIEW

Information security provides the basis for trust in the healthcare industry. A growing barrage of headlines about the most recent breaches indicate that health systems, healthcare providers, and service providers are losing the battle to protect their clients' health information.

Why is healthcare data valuable?

Healthcare data is more valuable on the black-market compared to other sensitive data breaches, the average Healthcare record sells for hundreds of dollars.

The number of breaches goes up year after year, in 2018 there were 365 breaches of more than 500 records affecting a total of 13,236,569 patients. *Can you afford take chances with your customer's data?*

HIPAA & HITECH

In the United States, compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) have increased the burden on healthcare providers, payers, clearinghouses, and business associates to protect their information. In Canada, organizations must wade through a mixture of provincial and federal Privacy and Security legislations.

When factoring in the cost and reputational impact of breaches and large fines, everyone is feeling the impact.

Whether non-profit or for-profit, the impacts of these reforms must be understood and addressed as part of effective and responsible patient care and financial management.

Security concerns and challenges

With the average breach exposing 1.3M people, you need to take every necessary precaution to protect your organization and consumers. The Healthcare industry, on average, under-spends on cybersecurity compared to other industries but the black-market value is a record high – it's no wonder why cybercriminals are focusing their efforts and increasing their sophistication with each attack.

Our Healthcare service provides you with an in-depth administrative, physical, and technical review of your current security posture.

We provide a comprehensive analysis of vulnerabilities, potential vulnerabilities, exploit information and, most importantly, business risk.

In the event that we discover an issue, we'll work closely with you to perform a root cause analysis to determine the best means for remediation.

The modern healthcare system continues to evolve from paper-based systems to complex inter-connected electronic ecosystems that contain Protected Health Information (ePHI).

This new landscape creates great opportunities for ubiquitous access and cost reduction, however it forces healthcare providers and businesses involved with healthcare to create strategies to address the following:

- ***Constantly evolving regulatory requirements***
- ***Stringent data security and privacy requirements***
- ***Collaborative exchange of information***
- ***Increased frequency of data breaches***
- ***Mobile medical devices***

Healthcare providers are being challenged with protecting confidentiality, availability, and integrity of this sensitive data. This includes:

- ***Complex healthcare infrastructures have diverse endpoints, networks, and applications***
- ***Compliance with applicable requirements such as HIPAA/HITECH, PCI, State Privacy Laws, and Provincial Privacy Laws***
- ***Electronic PHI can reside anywhere – on laptops, desktops, servers, removable media, and in the cloud***
- ***Controlling access to sensitive information can help prevent access by unauthorized entities***
- ***Encrypting sensitive information, including ePHI in transit or at rest***
- ***Securing sensitive data stored on mobile devices and removable media***
- ***Securing lost or stolen devices***
- ***Securing medical devices***

Healthcare Information Security Offerings

Online Business Systems has 20-years of experience within the healthcare industry and over 20-years of experience in the security arena.

We're working alongside healthcare providers to create sustainable information security governance programs and perform healthcare InfoSec risk assessments.

Due to the disparate nature of sensitive data and associated data management requirements, our Healthcare Information Security offerings are focused on the following key areas:

- ***Security and privacy governance and program management***
- ***Risk management methodology/assessments***
- ***Strategic remediation road mapping and activities***
- ***Penetration testing/ethical hacking***
- ***Third party risk management***

As a knowledgeable independent third party, Online Business Systems performs privacy and security assessments to certify our clients' adherence to local healthcare information security regulations, including HIPAA, HITECH, and jurisdictional Information Privacy Laws, drawing from other industry standards where necessary.

Our methodology provides a proven framework that can be tailored for unique business requirements as needed. Some of the key activities in our methodology include:

- ***Defining the Scope and Objectives of the assessment***
- ***Creating an inventory of where ePHI is maintained, accessed, and transmitted***
- ***Identifying Threats, Vulnerabilities, and Risks to ePHI***
- ***Assessing existing Administrative, Physical, and Technical Safeguards through an Interview, Observe, and Test Methodology***
- ***Developing a Report that highlights areas of High Risk to the business thus allowing the business to focus on the highest impact areas***
- ***Create meaningful and actionable recommendations for addressing identified risks***

Why Choose Online Business Systems?

Online Business Systems has the unique position of having both deep healthcare information technology consulting experience, spanning over 20-years, and extensive information security consulting knowledge with our consultants averaging 10-years of experience across many industries, including health care.

We take a collaborative approach by working closely with our clients to gain a strong understanding of their business model, critical data flows and repositories, network architecture, and systems/ applications that support their business.

This allows us to perform a thorough assessment of your security posture and, more importantly, puts us in a position to make recommendations that align with your business, your culture, your people, and your technologies. In the event that we discover an issue, we work closely with our clients to perform a root cause analysis to determine the best means for remediation.

We understand that information security is not black and white, but many shades of gray. By drawing on our vast experience in working with businesses, governments, and not for profit organizations, we position ourselves to take a pragmatic risk-based approach to information security to determine what controls, policies, and procedures best align for a particular organization.

online business systems

Online Business Systems
1.800.668.7722
rsp@obsglobal.com

About Online Business Systems

Founded in 1986, Online Business Systems is a Digital Transformation and Cybersecurity consultancy. We empower enterprise customers by enhancing their competitive advantage with improved business processes and secure information systems.

Our delivery, our people, and the Online culture of loyalty, trust, and commitment to mutual success set us apart. Today we have over 300 digital transformation and cybersecurity consultants throughout Canada and the US.