Saegis Shield

# Questions to Ask Before Selecting an IT Consultant or Vendor

For outsourcing IT or engaging third party vendors, ask the following questions to start to explore if the service provider is set up to protect information.

- How is data managed and where is data stored? Is it encrypted while stored?
- How is the data protected during transmission? Does the vendor encrypt data?
- How does a vendor authenticate users into their system?
- What is the audit reporting - can an unauthorized user access data without your knowledge?
- How does a vendor patch and monitor their systems?
- Does the provider use a robust / segregated back up system? Is it tested regularly?
- What are the data recovery procedures in the event of a failure or breach?
- Does the vendor's IT department have required expertise in information security and risk management?
- Can the vendor explain their cybersecurity practices / program?
- Have they been victims of a data breach or cyber-attack? Is there an incident management/breach response plan in place?
- Does the vendor have cyber insurance?

# Questions to Ask About Your Network Security

- Has the organization undertaken a system-wide security audit?
- Is there a robust plan in place to manage / prevent / respond to breaches and cyber-attacks?
- How often is the breach response plan reviewed?
- Are there policies in place that support the plan and are they enforced?
- Are there effective security controls in place?
- Are there security audits and regular system updates?

Saegis Shield

# Top 5 Cybersecurity Threats Facing Clinics

## Denial of Service

- A Denial of Service (DoS) attack is meant to shut down a machine or network making it inaccessible. For a clinic, this means can no longer connect to their Cloud or Internet service as it has been taken offline. This is an increasing threat as clinics are moving towards data centers in the Cloud and are more exposed and visible to hackers.

## Malware Attack

- Malware is malicious software that has been installed on devices and relies on simple human behavior such as browsing Internet sites or clicking on links where malware has been embedded and can be injected into a system.

## Social Engineering and Phishing

- Over 90% of incidents happen due to people. Hackers will by-pass security controls by hacking an individual directly.
- These are sophisticated attempts directed at individuals where the goal is fraud or data theft.

## Credential Stuffing

- Is an indirect and automated attack where hackers use stolen account credentials consisting of lists of usernames, email addresses and passwords to gain unauthorized access to accounts
- The best defense against an attack is to use Multi-Factor Authentication

## Unauthorized Access to PHI and Unauthorized Disclosure of PHI

- 30% of breaches is the result of unauthorized access or disclosure
- Healthcare is at particular risk due to insufficient security controls to protect PHI and the use of outdated/older technology

Healthcare organizations are targeted quite simply due to their legacy systems, lack of cyber awareness and business continuity planning.

Older technology poses challenges as more clinics move into the Cloud, PHI is extremely valuable on the dark web where nation states and organized crime can build their own data repositories to create profiles away from the original data source. Trained staff and implementation of cybersecurity best practices is the best defense against threats of cyber compromise.

The recommendation for all healthcare organizations is to invest in both a business continuity/disaster recovery plan and a breach response plan. These plans are essential to ensuring a fast recovery if a cyber incident were to occur and provides detailed information for staff to as to what mitigation actions are to be taken to report breaches and recover data.

**Please report a cyber incident to: cyberincident@cyber.gc.ca**

Saegis Shield

# Privacy Breach Guide

A privacy breach is the unlawful access, use, modification, disposal or disclosure of personal or personal health information. Examples of these include:

- Loss or theft of a device containing patient information
- Misdirected e-mails
- Cyberattacks
- “Snooping” on patient records

## The Privacy Breach 4-step process

### 1. Notify staff and the official health information custodians

If you suspect a possible privacy breach has occurred, you need to take immediate action and notify your manager or the appropriate staff member responsible for privacy operations. Where a breach involves a common/shared system between other healthcare professionals, the privacy officer or official health information custodian must notify those individuals or organizations of the breach as well.

If the breach involves personal health information (PHI) on a system shared by multiple custodians’, you need to notify all of them. If it involves a shared IT system or cloud provider, that means working with them as well.

### 2. Identify and Contain the Breach

Identify the individuals and organizations affected by the breach and determine what information may have been accessed, altered, destroyed or disclosed.

Next, focus on containing the breach. Change any usernames and passwords where the breach is the result of compromised accounts. If a system has been compromised, containing the breach may require shutting down the affected systems. Ensure that no copies of information were made. If copies were made, obtain evidence of the copies being securely destroyed by the individual or organization that made the copies.

Keep clear records of your activities and communications.

### 3. Notify Individuals, Privacy Commissioners, and Regulatory bodies

Individuals must be notified about a breach *at the first reasonable opportunity*.
Telephone, email, or by post are all acceptable forms of notification. If necessary, notification in person is also acceptable.

Saegis Shield

Notifications sent to individuals should include:

- The name of the individual or organization responsible for the unauthorized access;
- The date of the breach;
- A description of the nature and scope of the breach;
- A description of the PHI that was subject to the breach;
- The measures implemented to contain the breach;
- A statement that individuals are entitled to make a complaint to the provincial regulatory body or privacy commissioner;
- The name and contact information of the person in your organization who can address inquiries; and
- Where government-issued identification or banking/credit card information was affected, a statement to individuals to notify the appropriate government agency or financial institution that their accounts may have been affected.

Some breaches require that you notify privacy commissioners, or regulatory bodies within a short time. If you are a member of the Canadian Medical Protective Association (CMPA), we suggest that you contact the CMPA as an early step, particularly if there is a risk of patient harm or possible legal issues due to a loss of personal health information.

Refer to the *Notification and Reporting Requirements across Canada* section below, for your province's or territory's privacy commissioners' and regulatory bodies' notification requirements.

## 4. Investigate, Remediate, and Log the breach

Ensure that all notification requirements have been met for affected individuals, that you've reviewed the circumstances of the breach, and determined whether your policies and procedures were followed. Review existing policies and procedures regarding the protection of PHI and identify what improvements can be made, if found that they are ineffective.

Assess your cybersecurity controls and ensure that you have the right solutions in place. Work with your IT department and/or service providers to ensure that electronic safeguards are in place to protect against future unauthorized access.

All privacy breaches and incidents must be kept in a log, with a responsible person identified for maintaining the log. Logs should contain at a minimum the following information:

- The name of the individual or organization that caused the breach, where it is determined to be relevant, such as in the case of unauthorized access
- The date of the breach
- The nature, scope and cause of the breach
- The number of individuals affected by the breach
- A description of the PHI that was subject to the breach
- A summary of the steps taken to respond to the breach.