Cyber Liability: Minimizing the Risk of a Data Breach

In an age of electronic health records, stringent privacy regulations, and widespread concern about identity theft information security has become an increasingly significant risk management priority. Leaders of every type of healthcare entity should evaluate their overall cyber exposure, create a plan to secure confidential information and minimize the impact of a breach, and obtain appropriate insurance coverage.

Recent media accounts of unauthorized disclosures of protected health information (PHI) and other sensitive data underscore the importance of an effective information security program for all healthcare organizations. The following facts, reported in the 2016 Ponemon Institute article, Global Cost of Risk, relate to the scope of the problem in Canada:

- *54% of all breaches are due to hackers and criminal insiders.*
- *21% of all breaches are due to system glitches.*
- *25% of all breaches are due to human errors.*
- *The average cost of a breach for all business segments is $158 and increases to $355(per file) for healthcare records.*

The potential consequences of a data breach range from substantial monetary penalties (which are not necessarily covered by professional, property or general liability insurance policies) to negative publicity, disruption of routine, loss of public trust and possible patient harm, if medical data integrity is compromised. This article examines the causes of healthcare-related data breaches and suggests strategies for preventing and managing improper disclosures.

Data disclosures occur in a wide range of settings, including general hospitals, outpatient facilities, clinics, private practices, pharmacies and health plans.

Data Breach Causes

The causes of data breaches can be classified into five areas:

- *Theft of paper records or electronic media,* including computers and such portable devices as USB flash drives, personal digital assistants and smart phones.
- *Loss of paper or electronic records,* including laptops and storage media.
- *Unauthorized access to personal health information (PHI),* including external hacking, “malware” infection and illicit employee-related exposures.
- *Human or technological miscues,* including erroneous mailings and email or network server glitches.
- *Improper disposal of paper records,* generally involving errors made by a billing service or other vendor.

Risk Control Strategies

The following basic measures represent a useful starting point for discussions in your clinic on data breach prevention and response:

- *Perform a cyber-risk assessment/PHI inventory.* The critical first step in enhancing data security is to identify system vulnerabilities and account for how PHI is managed and secured. A variety of programs are available to assist in this

task, including the US Department of Homeland Security Cyber Security Evaluation Tool (CSET®) [http://www.us-cert.gov/control_systems/satool.html] and the OCTAVE® information security assessment approach. [http://www.cert.org/octave/]

- *Educate staff regarding the scope of federal and provincial privacy and notification requirements*. Basic Personal Information Protection and Electronic Documents Act (PIPEDA) and Privacy Act requirements should be integrated into employee orientation and training. Training sessions should explain the causes of data breaches and describe the consequences of neglecting to observe established data security policies, such as:
    - Disclosing PHI to anyone outside the organization who does not have a right to know.
    - Removing PHI from the facility without permission.
    - Failing to log out when leaving a workstation.
    - Sharing or writing down passwords.
    - Keeping laptops or storage devices in an unlocked vehicle or otherwise exposing them to theft.
    - Leaving confidential information displayed on a screen.
- *Secure record storage space.* To reduce the possibility of theft or sabotage, periodically re-evaluate and, if necessary, revise access control measures for restricted areas.
- *Implement a user monitoring system and effective access controls*. User logs should be implemented and carefully monitored. In addition, accounts should have suitably complex, regularly changed passwords and should lock automatically after a set number of unsuccessful log-ins.
- *Examine agreements with business associates regarding data sharing and security*. Contracts should expressly address PHI confidentiality issues in accordance with federal and provincial regulatory guidelines, applicable Standards of Practice for record keeping, and language should be reviewed and approved by legal counsel and IT specialists.
- *Adopt encryption technology*, which renders protected information unreadable and unusable in the event of a security breach.
- *Institute a post-breach response plan* in addition to complying with federal and provincial notification requirements. For ethical and reputational reasons, it is generally advisable to inform all affected parties of a data breach, even if such notification is not required by law.
- *Purchase cyber liability insurance* to address data- and privacy-related coverage gaps. Such specialized products can provide coverage for third-party liability (e.g., certain fines, indemnity payments and associated legal expenses), as well as for certain reimbursement costs and first-party losses (e.g. notification costs, system restoration expenses, credit monitoring for affected parties, if warranted).

Below is a self-assessment tool designed to aid healthcare business owners seeking to assess and enhance their data security risk control practices.

RISK CONTROL RECOMMENDATIONS – CYBER LIABILITY

Self-assessment Tool: Data Security and Patient Privacy

Areas of Concern

Risk Control Strategies: Staff	**Status**	**Comments**
Do staff members obtain thorough, up-to-date education and training about security- and privacy-related policies and procedures, and is this training: • Performed upon hire and annually thereafter? • Tailored to employees' job description? • Documented in employees' education files?		
Are employees encouraged to report procedural lapses and other events that may result in a security or confidentiality breach?		
Are employees held accountable for safeguarding patient privacy and confidentiality, and are they empowered to take appropriate action to secure sensitive information, including the use of encryption?		
Are information technology access and authorization lists periodically reviewed, and are individuals who no longer require access promptly removed?		
Is staff compliance with security policies and controls closely monitored and audited on a periodic basis?		
Risk Control Strategies: Physical and Technical		
Are basic security measures established and implemented, including locks on doors and windows, as well as surveillance/monitoring cameras for entrances, exits and areas containing sensitive information?		
Is an inventory maintained of all systems, devices and media that could potentially contain protected health information, including desktop computers, laptops, flash drives, printers, copiers, tablets and smartphones?		
Is there a visitor log to record: • Names of all visitors to patient care and business areas, including family members and contractors? • Time of visit? • Reason for visit?		
Are physical and electronic safeguards created and deployed to secure workstations and prevent inappropriate access to PHI, such as use of locked doors, cameras, keyed or fingerprint access systems, screen barriers, passwords, and firewalls?		
Are workstations located in secured and monitored areas and positioned correctly to protect against theft,		

unauthorized use and improper viewing of screens?		
Are employees reminded to sign off on workstations when they step away, and do monitors automatically switch to a neutral screen following a period of inactivity?		
Are policies and procedures established and implemented regarding security of office keys, as well as passwords, lock combinations and other access controls?		
Are locks re-keyed and combinations changed promptly when necessary – e.g., after a key is lost, a combination is compromised or a staff member departs?		
Risk Control Strategies: Security Policies and Procedures		
Is there a written data security plan, and is it regularly reviewed and updated?		
Are there rules governing the use of outside computers, as well as security standards for these computers?		
Are policies established and implemented regarding safe and secure disposal of electronic devices, as well as media potentially containing electronic PHI?		
Is electronic PHI removed from electronic equipment and media prior to disposal or offsite maintenance?		
Is there a logging process for business-owned mobile devices and media containing PHI, in order to track both where these devices are located and who has possession of them?		
Are records maintained of employees' personal electronic devices and media, if they may be used to access or store electronic PHI?		
Are security policies in place governing use of laptops and tablets, if these devices are used for purposes of patient documentation?		

This tool provides a reference for organizations to evaluate risk exposures associated with cyber liability. The content is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your clinical procedures and risks may be different from those addressed herein, and you may wish to modify the tool to suit your individual practice and patient needs. The information contained herein is not intended to establish any standard of care, serve as professional advice or address the circumstances of any specific entity. The statements expressed do not reflect a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice given after a thorough examination of the individual situation as well as relevant laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.