Week 8
Privacy and Security

Kevin Robertson, MBA

ACS-3801-050 Principles in Information Systems

Fall 2020

Week 8 Outline

- Reading: Chapter 9, Privacy and Security, p287– p321

  - Learning Objectives:
    - Distinguish Privacy, Confidentiality and Security
    - Review Privacy Acts
    - Describe and discuss Canadian Health Care Act
    - Able to identify threats to Health Care Information and IS caused by humans (intentional an accidental), natural causes and the environment
    - Understand the purpose and key components of the health care organisation security program
    - Discuss the increased need for and identify resources to improve cybersecurity in HC organisations
  - Summary

Introduction

- Privacy – the right to be left alone – out of the public
- In HIS Privacy is the right to limited access to patients health care information
- Unfortunately there is a large number of know and unknown breaches of the Protected Health Information
- Protection of PHI is a significant undertaking when operating HIS
- Electronic HIS open PHI to increased risk of being breached
- HIS users add to this risk by using personal devices

Privacy, Confidentiality and Security

- Privacy – individuals right to be left alone and limit access to their personal health information
- Confidentiality relates to the information shared with a healthcare worker during treatment is only used for the intended purpose
- Confidentiality relies on Trust between patient and carer
- Security – systems that are in place to protect HIS
- Protect against unauthorised access to PHI and also protect IT assets (networks, hardware, software)

Legal Protection of Health Information

- Many forms of control, policy and practices exist to protect patient information and privacy
- Regional (provincial/state), Federal, and local
- Ethical and professional standards published by medical associations
- Infractions can lead to federal/provincial prosecution

Canadian Health Act

The Canada Health Act (CHA or the Act) is Canada's federal legislation for publicly funded health care insurance.
The Act sets out the primary objective of Canadian health care policy, which is "to protect, promote and restore the physical and mental well-being of residents of Canada and to facilitate reasonable access to health services without financial or other barriers."

https://www.canada.ca/en/health-canada/services/health-care-system/canada-health-care-system-medicare/canada-health-act.html

Canadian Health Act - Principles

- Public Administration, Provincial insurance providers accountable to expenditures (costs)

- Accessibility – Canadian residents must have access to all medical service without charges or additional costs

- Comprehensiveness -programs insure patients against all medical necessary service

- Universality – Canadians have access to medical necessary services without needing additional insurance

- Portability – Canadians covered outside their province of residence

Canadian Health Act - Objectives

1. To ensure that every Canadian has *timely* access to all medically necessary health services *regardless* of his or her ability to pay for those services.

2. To ensure that *no* Canadian suffers *undue* financial hardship as a result of having to pay health care bills

https://sencanada.ca/content/sen/committee/372/soci/rep/repoct02vol6part7-e.htm

Personal Information Protection and Electronic Documents Act (PIPEDA)

Canadian Legislation to protect patient information and its use

There are a number of requirements to comply with the law. Organizations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy.

Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, they must obtain consent again. Personal information must be protected by appropriate safeguards.

Some regional exceptions, some provinces have equivalent laws and regulations

Federally related organisations always subject to PIPEDA

Patient Healthcare Information

- Demographic
  - Name (e.g. first, second, surname)
  - Address
  - Date of Birth
  - Post Code
  - Gender Category
  - Provincial Health Card Number
  - Next of Kin
  - Ethnic origin

- Care Plan Specific
  - Blood type
  - Events
  - Visits (MRN – Medical Record Number)
  - Care plans
  - Test Results
  - Allergies

Legal Obligations and Penalties

- Fines in excess of $50K per day for breaches
- Audits and Reviews
- Patients can ask to know who has looked at their personal PHI
- Expectations are that HIS service providers can report on use of patients data
- Methods to allow patients to raise concerns and lodge complaints

Threats to Health Care Information

Three Types

1. Human Tampering Threats

2. Natural and Environmental (disasters)

3. Technology factors and malfunctions

Human Tampering Threats

- People are the weakest link in any system
- Intentional or unintentional
- Internal or external to the HIS
  - Knowing disclose patient information vs accidental disclosure
  - Without authorisation, theft, destruction, changing
  - Employee, hacker or other criminal activity
  - Email payload, virus, direct attack

- Systems should enforce security and limit access to only functions needed
- Procedures, policies and practices must be implemented

Human Tampering Threats

- Viruses – contaminated software or electronic documents
- Trojans – look like normal files type containing malicious code
- Spyware – tracks activities, assisting the hacker to gather information, user ids, password, bank details etc.
- Worms – software code that replicates itself in computer systems and migrates throughout the organisation infrastructure
- Ransomware – cripples access to organisation data a special key is required to decrypt the data, payment made via untraceable mechanisms like “bitcoin”

Human Tampering Threats

- Losing a laptop with PHI loaded
- Accidentally opening an email from a friend with a picture or document containing a payload
- Making password very generic and simple “123456”
- Generic account name vs named person
- Mis-using a supplied device for personal use
- Not securing laptop to a secure docking station
- Not securing workstation when leaving their desk
- Workgroup organisation allows users to view other users machines
- Faxing data to the wrong fax number

Natural and Environmental (disasters)

- HIS organisations must have a plan to deal with large scal disasters
- Major environmental dangers floods, fires
- Disaster management, failover systems
- What happens when failover fails?
- Pandemic – what happens if no staff available?

Technology Malfunctions

- Infrastructure and software failures, hard disk failures
- Backup policies and data restoration procedures
  - May require business to maintain written documents
- High availability systems with redundancy (expensive)
- How long can a service actually be down before it is critical
- Use cloud services, critical data saed on network drive/DBMS

Complexities for HIS Providers

All businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation).

Using Cloud based services raises concerns over where the data resides, encryption in transit and logical flow of data from one site to another

Complexities for HIS Providers

- Personal Devices (Bring Your own Device)
- USB Devices – Flash drives
- Excel Spreadsheets
- Printing reports
- Availability at alternative sites
- Audit Logging and Reporting

HIS Security

- Protection of HIS information is the responsibility of the Security program
- Its function is to identify potential threat and implement procedures, processes and practices to mitigate the risks to HIS information
- Difficulty: balancing the cost of security to the need
- How to calculate the cost of the likelihood of a successful attack against the cost of actually protecting against it
- Difficulty to access the actual cost of not having access to HIS for 1 hour or 1 week

HIS Security

- Also, availability vs the layer of protection (security) put in place to mitigate risks, too much security makes it difficult to access the data at the right place and at the right time

- Too little security means systems and PHI are at risk and the organisation is liable for any breach of patient data security

- Comprehensive security practices need to be in place but must be relative to the risk (often Security and Risk Management are closely related)

ONC Security Process

1. Lead your culture, select your team and learn
2. Document your process, findings and actions
3. Review existing Security of PHI
4. Develop an Action Plan
5. Manage and Mitigate Risks
6. Attest for Meaningful Use Security Related Objective
7. Monitor, Audit, and Ongoing Security Updating

Lead your culture, select your team and learn

- Designate Security Office to lead, develop and implement security practices
- Discuss security requirements with vendors/developers to be implemented into HIS
- Hire qualified security professionals to support practice
- Use tools to understand security threats and vulnerabilities
- Continuously refresh your knowledge of security standards and liabilities
- Promote a culture of protecting patient privacy and security patient information. All staff are responsible.!

Document your process, findings and actions

- Policies and procedures
- Completed security checklists
- Security Training materials and course completion
- Security Risk Analysis Reports (TRA – Threat Risk Assessments)
- Application Audit logs relative to security access
- Risk Management Action Plan for the organisation with timetables, activities and objectives
- Security breach incident management

Review existing Security of PHI

- Risk analysis assess potential threat and vulnerabilities to the confidentiality, integrity and availability of PHI (application specific)

  - Identify where PHI exists
  - Identify potential threats and vulnerabilities
  - Identify risks and their associated levels
    - Likelihood (Low, medium, high)
    - Risk level (High, med, low)

Develop an Action Plan

An action plan is needed to detail activities to remediate security risks and vulnerabilities

- Administrative safeguards
  - People focussed, security officer, staff training
- Physical safeguards
  - Uncontrolled area physical access issues
- Technical Safeguards
  - No/limited audit capability
- Organisational Standards
  - No breach reporting process in place
- Policies and Procedures
  - Generic documentation, ad hoc practices

Refer to p310 in text book for more detail

Manage and Mitigate Risks

- The Security plan needs to be implemented and used by all staff
  - Implement Plan
  - Prevent breaches by educating and training workforce
  - Communicate with patients
  - Update your service business agreements contracts

Attest for Meaningful Use Security Related Objective

- Meaningful use, essential using HIS to provide enhanced patient care
- A program was implemented in USA to promote meaningful use and make payments to providers increasing use of HIS
- Satisfying security component of program relies on amplecting a plan and reporting progress

Monitor, Audit, and Ongoing Security Updating

- Security officer, IT administrator(s) and vendors to ensure the organisations monitoring and audit functions are active and configured appropriately
- Auditing ad Monitoring are necessary to answer the question of “who, what, when, where and how”

Cybersecurity for Todays Wired Environment

- On average HIS providers spend less than 6% of their budget on security
- Modern technology has exceeded the ability of older legislations to keep up with the connected HIS
- Cyberattacks are on the increase
- HIS are seen as one of the biggest targets of external threats
- Problem more entry points into the HIS landscape across many service areas
- Proliferation of mobile devices

Protect Mobile Devices – Managed Devices

- Ensure mobile devices are equipped with strong authentication and access controls
- Ensure laptops have password protection
- Enable password protection on mobile devices
- Protect wireless transmissions from intrusion
- Do not transmit unencrypted PHI across public networks , use VPN
- Encrypt data on the device (bitlocker technology)
- Do not allow devices that cannot support encryption
- Develop and enforce policies when devices can be removed form the facility
- Take care to prevent unauthorised viewing of the PHI displayed on the mobile device

Maintain Good Habits

- Uninstall all unnecessary applications not used for the job
- Control install of apps do not allow basic installs
- How does the vendor update their apps?
- Disable remote file sharing and remote printing within the OS
- Automate software updates (weekly)
- Monitor for critical updates and patches immediately and act accordingly
- Manage user accounts closely (create/delete)
- Have standard practices for position terminations
- When disposing of hardware cleanse appropriately
- Archive old data
- Use managed devices, controlled by ICT services

Other Actions

- Use Firewall to protect all internally available services
- Install and maintain anti-virus software
- Plan for the unexpected
  - Regular backups and testing restores
  - Automate backups
  - Cold storage
  - Have a recovery plan and available externally

Control Access To PHI

- Grant PHI access to only those who need to know
- Set file access permissions
- Use account management tools to authorise user roles
- Use role based accounts, assign staff to role (or multiple roles)
- Use the application to control where information can be accessed from and who by using scheduling

Use Strong Passwords

- Don’t use easy to remember names!
- Use password policy to detail minimum requirements
  - Minimum of 8 characters
  - At least one upper case character
  - At least one special character (“!@#$%^&*)
  - Do not use date of birth, pet names, SIN, Gamer Tag
- Technology – use Two Factor Authentication if possible
- Combinations – finger print and password
- 90 Day forced changing with no repeats last 5 used
- Provide efficient password change practices

Limit Network Access

- Encrypt wifi networks
- Prohibit staff from installing software (unless approved)
- Prohibit casual network access
- Enforce procedures to control the creation of network accounts
- Remove peer-to-peer applications
- Enforce vendor access rules and policies

Control Physical Access

- Limit the ability to access devices attached to the network
- Avoid open access terminals for the public
- Disable USB drives on computers
- Remove CD-Blue-Ray disk readers
- Install network management tools to detect “new’ devices being added to the network and isolate until approved
- Document and enforce policies limiting physical access to devices in information
- Locked rooms, manage keys, restrict removal of devices from secure area

National Institute of Standards and Technologies (NIST)

- USA based organisation responsible for “enhancing security and resilience of US critical Infrastructure”
- The NIST Framework was defined to support this responsibility
  - **The Core:** 5 functions “Identify, Protect, Detect, Respond and Recover” detail a strategic view to management of cybersecurity risk
  - **Framework Implementation Tiers:** characterises the organisations actual cybersecurity practices compared to the framework (level 1-4)
  - **Framework Profile:** details the results of reviewing the organisation against the categories and sub categories

Summary

- Privacy – the protection of an individual
- Confidentiality – the understanding that the patients interaction and information shared with a care giver is sacred
- Patient Health Information must be protected and only used with approval by the patient
- Governments have put in place legislation and legally binding regulations to protect patient data
- Implementing security measures to protect HIS information
- The weakest link is people, either accidentally or on purpose
- A security plan is needed and must be constantly updated