Examples of Commonly Used Security Safeguards

Administrative Safeguards

- Access to personal health information and access to any place or system where personal health information is kept must be restricted to individuals who are authorized to use, modify, transform, disclose, dispose or destroy personal health information to perform their assigned duties. Employees and other information users must be authorized to access, maintain, change, use or distribute information. Authorization for each information user should be based on the 'need to know' of that individual.

- Security checks may need to be employed to ensure that individuals in key employee positions are screened. This includes background checks and taking oaths of confidentiality, where necessary. Screening of personnel should be done on a regular basis, and criminal record checks may be appropriate and required in some cases. For example, health care providers like hospitals and nursing homes should require every successful applicant for employment and every new volunteer to provide a criminal records check.

- All systems programmers, network/LAN technical staff, ID administrators, file and mailroom staff that have privileged access to the work environment and have to be "trusted".

- Information access privileges should be reviewed, modified or revoked as necessary when:
  - an employee is transferred by appointment, assignment or secondment;
  - an employee commences an extended period of absence, including maternity, medical, military or community service;
  - access privileges have not been exercised for a period of time; or
  - the employment or contract of the individual has been terminated. Upon termination:
    - the individual should be debriefed with respect to ongoing responsibilities for the confidentiality of Trustee information;
    - access privileges (system passwords, user ID's, combinations, etc.) to systems, restricted access zones, and IT facilities should be revoked; and
    - all security related items (badges, keys, documents, etc.) issued to the individual should be retrieved.

- To ensure that parties accessing information are who they say they are, the identity of any individual who accesses, uses, modifies, transforms, discloses or disposes of health information must be verified and authenticated prior to access to information being granted.

  The most common form of this safeguard in an electronic environment is the use of passwords. However, it could also include requiring proof of identification using tokens, biometrics, challenge/response scenarios, one-time passwords, digital signatures and certification authorities.

  Authentication passwords or codes must be:
  - generated, controlled and distributed in a manner which maintains the confidentiality and integrity of the code or password;
  - known only to the user of the identifier;
  - either pseudo-random in nature or verified by an automated process designed to counter triviality and repetition;

  - at least 7 characters in length;
  - one-way encrypted for storage in the computer system subject to a history check to preclude reuse;
  - prompted for manual user entry when using automatic or scripted log-on processes;
  - changed at least every 90 days; and
  - a mixture of characters, both upper and lower case, numbers, punctuation and special symbols.

- Records should be kept identifying all instances of access, use, modification, transformation, disclosure or disposal of individually identifying diagnostic, treatment and care information.

- Records must be kept of all instances of unauthorized access, use, change, deletion/disposition or disclosure of personal health information.

- Procedures, policies and practices must be implemented to restore, replace or re-create personal health information that has been damaged, lost or destroyed either accidentally or deliberately.

- Policies, procedures, practices and other safeguards must be implemented to minimize the risk from unauthorized access to, or unauthorized use, modification, transformation, disclosure, disposal or destruction of personal health information, and also to ensure accuracy and completeness of personal health information.

  Each Trustee must have or adopt policies and procedures that facilitate the administration of PHIA and the Regulation. Policies and procedures of Trustees should cover all aspects of administering the act but are particularly important in the area of ensuring the confidentiality and security of personal health information in their custody or under their control and the privacy of the individuals who are the subjects of that personal health information.

  The policies and practices suggested in this document could form the basis of what is adopted by a Trustee. Larger Trustee organizations must have substantial policies and procedures in place covering the collection, use, disclosure, security, retention and destruction of personal health information. These should be periodically reviewed and adjusted as needed to comply with any changes applicable laws, such as PHIA. Regulated health professionals may be guided by standards for health records or for the disclosure of personal health information published by their regulatory bodies.

  For example, By-law #11 Standards of Practice of Medicine of the College of Physicians and Surgeons of Manitoba contains, among other things, requirements for their membership in respect of patient records and privacy and confidentiality.

  The policies and procedures should be in writing, current, and available to all staff. Policies, procedures and penalties for non-compliance should also be outlined in contracts for service providers.

Physical Safeguards

- In addition to restrictions on who can access personal health information, access to the facility, offices, information retrieval equipment and systems and information stores must be

controlled to ensure that access is granted only to individuals with authorization for such access.

These controls relate to mechanisms in a computer operating system, hardware unit, software package, file room or mailroom. This is typically a password for systems access but may include card locks and physical security access systems such as keys, digital card keys and cipher lock barriers.

- Physical security safeguards to maintain access control can range from anti-theft systems such as bolting equipment to the floor in secure rooms, locked desks and cabinets.

- Smaller Trustees with little personal health information in electronic form should concentrate on physical security measures (locked rooms or cabinets, adequate access controls for employees and the public and sound disposition measures for the information). Larger Trustees with sensitive personal health information in a variety of forms and formats will have to take a wider range of security measures based upon the threat and risk analysis conducted.

- Stringent protection measures should be applied to personal health information with a high level of sensitivity and with a greater possibility of causing damage to an individual if it is accidentally disclosed, stolen or finds its way into unauthorized hands.

- For less sensitive personal health information where the risk of compromise or unauthorized access is low, a Trustee may only need to put in place lower grade security measures.

  Examples of these would be unlocked cabinets in a controlled area that are locked at night; computers being kept behind service counters, with screens not visible to patients/clients other than the subjects of the information; and computers accessed through restricted authorization codes.

  The OIPC Investigation Report H2003-IR-003 (Theft of Computers) investigates the theft of computers that were connected to the electronic medical record system within a clinic. The data server that stores all the health information was in a locked room and was not removed. It was the practice of the clinic that no health information was saved on individual computer hard drives. Thus there was no privacy breach just a significant loss of computer hardware. The clinic had taken steps to increase the level of physical security by installing a monitored alarm system and strengthened the rear exit door.

Technical Safeguards

- See also Administrative Safeguards and Physical Safeguards for related information about access controls and authentication passwords and codes and other forms of user verification.

  All methods of communication of personal health information must be secure from unauthorized access, including eavesdropping, interception and diversion.

"All methods of communication" includes verbal communication, transmission of written documentation, telephone, cellular phone, fax, e-mail, video and audio communication or any other form of electronic communication.

"Eavesdropping" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques such as remote monitoring of conventional telephone or cellular phone conversations, voice mail or text messaging, gain access to personal health information.

"Interception" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques gain access to health information ex: by interrupting the flow of information over a transmission line, through the use of electronic or other means.

"Diversion" occurs when the direction of the flow of personal health information is changed inadvertently or through the use of deceptive techniques so that an unauthorized recipient can gain access to it.

- Identification and authentication safeguards to monitor security systems and procedures may be needed. These include virus scanners, firewalls, monitoring operating system logs, software logs, version control and document disposition certification.

- Encrypted storage and transmission is necessary for particularly sensitive personal health information.

  In OIPC Investigation Report H2007-IR-002 Alberta's Privacy Commissioner determined that password protection is not sufficient to protect personal information and that all portable media must have a second layer of protection - namely encryption.

  "Encryption" refers to the technique or process of transforming information from human readable form to a meaningless form using mathematical number theory (a computational algorithm). Encryption may be used for an entire record of information, in which case it must be decrypted before it can be used at all.

  Many computer systems keep identifiable information stored in encrypted form to prevent casual access to information. Secure applications would decrypt the information prior to providing access to authorized individuals performing specific activities.

  Encryption can be used to transform a personal identifier to a unique, but anonymous identifier. Anonymous identifiers allow processing of discrete person level records to analyze information across time, data sources or geographical areas for such purposes as measuring utilization, health system performance, and health outcomes or program evaluation.

  Encryption may be hardware or software based and is usually "key" based. A Public Key encryption system uses a publicly accessible and widely understood encoding/decoding process, a set of publicly available keys, and a secret matching set of private keys.

  A "key" refers to a string of digits and/or characters used to encrypt or decrypt a message. The level of security often depends upon the length of the key.

- All systems hardware and software must be secure from inappropriate access, accident, misappropriation, viruses and systems failure.

- Put in place disaster recovery safeguards. These can range from the use of on-site diskettes/tapes to replication with an external system and duplication (ex: photocopiers) on other media forms with possible off-site storage facilities.

- Other related safeguards include the use of redundant or fault tolerant equipment such as disk shadowing/mirroring, dual systems, hot backups and alternate routing. These safeguards are typically hardware based but require software/procedures to manage the environment.

- Personal or health information should not be stored on mobile computing devices unless absolutely necessary. Consideration should be given to other technologies that allow secure, remote access to the required network and data instead. If necessary, there should be a privacy impact assessment (PIA) or threat risk assessment completed prior to implementing mobile computing. If personal information or personal health information is required to be stored on a mobile device, keep only a minimum amount based on the business need and use encryption to protect the data as password protection alone is not sufficient. It is important to periodically check practices against policies to ensure they reflect reality and remain effective. As well, specific training on mobile computing must be provided to staff to ensure they understand the risks and how to protect their equipment.

For information on security standards, refer to Canada's Health Informatics Association COACH Guidelines for the Protection of Health Information. (http://www.coachorg.com)