Maintaining Confidential Records

Description:

This tool provides recommended practices for employees and managers on how to maintain confidential records.

How it can be used:

Surprisingly, problems with confidentiality may occur where you least expect it – with people just being sociable. For example, it is easy for employees to slip when they talk about what they are working on to a co-worker or a spouse.

Accreditation requires that organizations safeguard confidential records; a critical responsibility that relates to both electronic and paper information. Health organizations must understand the confidential information it holds, control who has access to that information, and put in place measures to protect that information. Follow the recommended practices in this tool to guide both your managers and your employees.

Confidential Information is any information identified as personal, sensitive, or confidential that would identify a person, their health record, education record and any other non-public information as specified in federal or provincial laws or your organization's policies.

Examples are:

- Social Insurance number
- Physical description
- Home address
- Home telephone number
- Ethnicity
- Education
- Financial information
- Performance evaluations
- Medical and employment history

All confidential information must be safeguarded using the appropriate level of physical and electronic security. When working with confidential information, each employee takes on the custodial responsibilities for that information.

Recommended practices for maintaining confidential records can be organized by four key functions:

1. **Identify**: Identify and inventory where confidential information is stored, processed, and transmitted.
2. **Protect**: Protect confidential information against unauthorized access, use, loss, and damage.
3. **Communicate**: Communicate your responsibility for safeguarding confidential information.
4. **Maintain**: Maintain up-to-date confidentiality, integrity, and access measures.

In addition, employees and managers have different responsibilities. The following table describes the roles of employees and managers in relation to the four key functions.

Employee	Manager
Identify: *Identify and inventory where confidential information is stored, processed, and transmitted.*	
Emails, electronic documents, paper files, desktop computers, laptops, cellphone, hard drives and memory sticks, disks, zip drives, external hard drives, CD/DVD, USB devices, shared drives, etc.	Identify and inventory all systems that contain, process, and transmit confidential information. Identify the functions and approve authorization for staff members who need access to confidential data.
Protect: *Protect confidential information against unauthorized access, use, loss, and damage.*	
Do not share personal access codes or passwords. Install and maintain all security and antivirus software updates on all computers/laptops/software. Keep portable storage devices secured. Do not leave computer equipment unattended unless system is logged out or locked. Use boot-up passwords for all computer systems. Enable screen savers with locking passwords. Never open an attachment without verifying it with an antivirus program. Position monitors and printers so that others cannot see or obtain confidential or sensitive data. Make sure you have a secure online connection. Restart your browser when finished in case information is stored in the browser's cookies. Change passwords regularly and when someone who had access leaves the job or a key is lost or stolen. If working at home, make sure to keep the system and data secure from unauthorized access.	Keep all employee files in locked file cabinets, with regular employee files apart from the employee medical files. Medical information must be kept secure with access limited to those that need the information. Ensure there is physical security surrounding equipment, programs and files and that copies of all programs and data files are maintained in a secure location away from the computer and primary records. Social Insurance Numbers should be used only where they are absolutely necessary. Allocate appropriate resources to protect confidentiality and security of electronic and printed information in work areas. Grant employees only the appropriate level of access necessary for them to work with confidential data. Maintain records of who is authorized to access confidential data. Consider a log. Provide resources for training for all employees with access to confidential information.
Communicate: *Communicate your responsibility for safeguarding confidential information.*	
Promptly report any possible unauthorized access, use or loss of information. Never send confidential information using non-secure applications such as text, Facebook or regular e-mail.	Communicate management's responsibility to protect the privacy of all staff and clients. Ensure employees understand and follow procedures that protect confidential information.

Employee	**Manager**
Do not send sensitive information to e-mail accounts other than those already authenticated. Always use an authenticated and approved protocol for remote communication when accessing critical servers or resources containing personal or confidential information. Get appropriate authorization before taking any equipment off-site.	Ensure employees do not discuss confidential information unless legitimately required. Notify security when new systems containing confidential information are implemented. Implement and administer standards that: - Maintain and manage systems which contain, access, or transmit confidential information. - Verify that background checks are conducted for anyone accessing confidential data or systems. - Show how to safely retain and destroy all records containing confidential information. - Identify and prioritize the impact of downtime on operations and systems (business continuity). - Preserve information in the event of disasters.
Maintain: *Maintain up-to-date confidentiality, integrity, and access measures.*	
Securely dispose of unnecessary confidential information in an approved manner. Remove any confidential and private information that it is no longer needed to minimize liability in case the computer becomes compromised. Seek authoritative advice on disposing of equipment and data. Ensure that confidential, sensitive, or personal data is properly cleaned from internal disks or removable media prior to disposal or transfer to others.	Maintain inventories and confidentiality, integrity, and keep access security measures up-to-date. Maintain an up-to-date registry of all systems containing confidential information. Conduct an annual risk assessment on all systems containing confidential information. Maintain documentation and training for employees with access to confidential data. Maintain procedures for upgrading and updating the information systems. Ensure information systems are managed according to recommended security practices.