Office of the Information and Privacy Commissioner of Alberta

Cause of Breaches and Breach Prevention Recommendations

Overarching recommendations: 1) Limit the amount of personal information collected to that which is reasonably needed to meet your business requirements; **2)** Develop procedures involving the handling of personal information with privacy protection in mind, including breach notification procedures, and develop policies to support the procedures established, **3)** Train staff to thoroughly understand the importance of protecting personal information - have staff sign a confidentiality agreement acknowledging their obligation to protect personal information; **4)** Ensure proper contract controls are in place binding contractors to your organization's privacy policies, procedures including training, and breach reporting requirements; and **5)** Keep personal information only as long as is needed to meet business and legal requirements then securely destroy the information. **6)** Update policies and procedures annually.

Causes of Breach	Recommendations on How to Prevent a Breach
Human Error • Email, mail and faxes sent to the wrong individual(s) • Email address viewable in the "CC" line to all individuals in a mass email, emailing too much or unauthorized information • Faxes sent to an unsecure fax • Mail or couriers sent to the wrong person • Documents lost on public transport or gone missing • Documents disposed of in the trash, or intended for shredding and disposed of improperly • Computer hard drive given to the wrong person • Verbal disclosure	• Establish email procedures that involve double-checking the address to ensure it is correct prior to sending. For mass emails double-check that all emails are contained in the bcc section. Ensure staff are aware what they can and cannot email. • Develop a secure fax procedure that requires double-checking the fax numbers prior to sending and use a fax cover sheet with a privacy disclaimer and your contact information for a misdirected fax. Use pre-entered numbers for routine faxes and double-check to ensure you are selecting the correct key prior to sending. Confirm the recipient fax machine is secure and confirm receipt of the fax. • Use window envelopes to avoid sending a letter to the wrong address. • Instruct couriers to deliver packages directly to the intended recipient or a secure location and to return the package where your instructions cannot be carried out. • Establish secure disposal procedures for personal information including secure recycling and shredding – do not dispose of personal information in the garbage. • Establish procedures when electronic equipment containing personal information is picked up or delivered that require verifying the identity of the individual to avoid giving the equipment to the wrong individual. • Establish robust security controls for disclosing personal information verbally. Gear the complexity of the security questions to the sensitivity of the information
Theft • Information taken by a former employee • Office and car break-ins resulting in the loss of files and computer devices, including laptops and hard drives	• Develop employee termination procedures, which include terminating access to electronic systems, return of electronic equipment and return of keys and access cards to avoid loss of personal information. Upon termination establish a process where employees are reminded on termination that they must not remove any personal information without the express written consent of the organization and to do so is a violation of the law. • Ensure employees understand the importance of protecting personal information when taking work home and provide secure means to facilitate the transport of personal information by password protecting. Encrypt electronic devices containing personal information (including laptops) with strong encryption and ensure employees do not store personal information on hard drives. Develop policies that address taking work home and transport of electronic devices. • Ensure electronic and paper records are properly secured in offices and not left in employees' cars and instruct employees to never take paper files out of the office for any reason. • Store paper records in locked file cabinets and lock up portable electronics (or secure with locking devices).
System Compromise • Targeted network attacks by external hackers seeking to extract large amounts of data or ethical-hackers hacking a system • Information viewable on the Internet due to a system upgrade • System glitch misdirected faxes	• Ensure proper information technology security is in place. • Test the security of the system for vulnerabilities during and following any modifications. • Test and monitor the security on a routine basis to identify weaknesses.
Inadequate Access Control • Improper access controls to electronic and paper files resulting in the files being accessible to those not authorized to have access	• Segregate files on electronic systems containing personal information and establish access controls. • Ensure e-files can be audited and audit routinely to assess compliance. • Determine whether there is personal information stored on obsolete databases. • Establish access controls that limit access to personal information on a need to know basis and audit to assess compliance. • Adopt a clear desk policy and ensure paper records are locked away in a secure location.