

# RISK CASE STUDY

## Case: Breach of Personal Health Information

### Abstract:

A program director inappropriately accessed person health information. The director's employer - a community health centre - lacked a robust process to train staff with respect to privacy of personal of health information and failed to conduct health record access audits.

### Case summary:

During the course of a 20-year employment term at a community health centre, a senior program director repeatedly accessed the personal health information of numerous family members and social acquaintances. The organization was informed of the breaches following a complaint by a member of the involved employee's immediate family.

### Medical legal findings:

Expert review of the case was critical of the involved community health centre, indicating that the involved employee appeared to have no understanding of client confidentiality. Further, it was noted that a review of the employee's employment record provided no evidence to indicate that the employee had received appropriate training with regard to the organization's policies and procedures related to client confidentiality. Expert review questioned the community health centre's internal audit processes, given the organization's apparent failure to identify the privacy breaches prior to the receipt of the complaint.

### Reflections:

Reflecting on your practice as well as your facility's policies, procedures and processes:

1. With respect to staff training and orientation, discuss whether small community organizations and clinics should be held to the same privacy standards as large hospitals. Would lack of resources be sufficient justification for not implementing necessary controls to minimize and identify privacy breaches?
2. Discuss your organization's privacy policy. Does it clearly define the possible consequences of breaching a patient's personal health information? Does it include a standardized privacy breach response protocol? Discuss the role of policies and procedures in legal and regulatory body investigations.
3. Does your organization have a standardized privacy breach response protocol? Is the protocol effective? Is its effectiveness reviewed following each privacy breach?
4. Discuss the role of audit logs for internal quality control purposes as well as following a suspected privacy breach. How long are audit logs retained?
5. Discuss your organization's threshold for patient and external notification following a privacy breach, specifically who is to be notified and within what timeframes?



This is a resource for quality assurance and risk management purposes only, and is not intended to provide or replace legal or medical advice or reflects standards of care and/or standards of practice a regulatory body. The information contained in this resource was deemed accurate at the time of publication, however, practice may change without notice.

### Key Words:

Privacy Breach

Information  
Technology

Personal Health  
Information

Community Health  
Centre