



Privacy 301 – A Health Information Technologist Perspective on Privacy Breaches & Responses

Michael Whitt and LeRoy Brower

Michael Whitt is a partner with the Borden Ladner Gervais in Calgary, Alberta; LeRoy Brower is the Director, Health Information Act, Office of the Information and Privacy Commissioner, Alberta.



Introduction

In this continuation of a series (back by popular demand!), we discuss the types of privacy breaches which can occur,

describe some that have occurred, and through the FAQ format, answer some interesting questions about privacy breaches, security, situational analysis of breach scenarios, and some proposed responses.

It must first be noted that “privacy breaches” are not necessarily the same thing as “IT security breaches”. For instance, over-broad collections, use for unauthorized purposes, and data-matching outside of the scope permitted by legislation are all breaches, none of which has to do with “security”. It should also be noted that breaches can occur outside of the direct control of the custodian or entity with primary responsibility for health information, and that the responsibility remains the responsibility of that entity (which may or may not have recourse against the entity which could have controlled the circumstances of the breach).

In our estimation, most privacy regulatory schemes are successful when they motivate the custodian, collector, or responsible party to examine and consider impacts of systems, both IT and workflow or procedural systems, on the exposure of data subjects to new risks. Data subjects can be patients, care providers, or ancillary personnel about whom data is collected. When design and implementation of such systems contemplate AS A SEPARATE AND SPECIFIC CONCERN the impacts upon data subjects’ personal information privacy, most conceivable threats or risks can be avoided or mitigated, and breach situations can be predicted and provided for, thus having the desired effect of reducing or eliminating those risks while permitting the enjoyment of desired system benefits (both by the operator and the data subjects).

Having said all of that, in these “early days” of privacy regulation in the healthcare sector, most breaches that we are experiencing (and advising on, analyzing, or investigating and prosecuting) have to do with IT security breaches and, at this stage, fairly superficial concerns (the concerns have more to do with repurposing, disclosure to third parties, and improper retention and destruction processes than with scope of initial collection, notification, knowledge and form of consent, or proper PIAs).

Examples of the types of breaches which are, sadly, becoming commonplace, include:

- surplus or redundant equipment which includes improperly erased media (tape drives with surplus data tapes with patient information sold in BC; computer equipment sold with hard drives having patient and care-giver information);
- improper handling of back-up media (physician leaving partnership taking copy of back-up data to new practice “to preserve his access to his patients’ data”; employee leaving back-up disk on bus on way home);
- stolen computer equipment, including personal information (laptop stolen from office, computers stolen from physician premises);
- unexpected disclosure of personal health information (deceased’s doctor’s staff dropping paper files off at hospital reception area);
- outsourcing of IT work to insecure or off-shore service providers under inadequate contractual or other legal control;
- insecure systems being hacked (departed employee system identifiers not being terminated at departure, use of “default” system passwords, id’s and passwords being used by hackers to log into physician office systems and manipulate files);

- electronic medical record data back-up tape is stolen from front seat of car when doctor's staff stops at a store on the way home;
- health information viewed on computer of another business located in the same building as medical clinic, due to wireless system not being properly implemented with necessary safeguards to reasonably protect the information;
- medical records found on second hand computer previously owned by transcriptionists who had returned the faulty computer for warranty;
- paper health records being lost or stolen while health services being provided in the community;
- unauthorized access - health service provider accesses electronic health record to obtain information about ex-spouse; health service administrator accesses electronic health record to obtain information useful in second job and for personal reasons; student accesses electronic health record to obtain information about people from the student's hometown;
- transportation security - data tapes and other health information media being lost somewhere while off-site or in the shipping process; and
- healthcare web-portal accidentally publishes identities and information of prior page-users; password-protected pages with personal health information of patients show up on Google™ search;

Most of these examples, when viewed from the perfect perspective of hindsight, are obviously best prevented and dealt with by proper prospective analysis and system design (in other words "a stitch in time saves nine"). Policies and procedures dealing with proper, thorough and certified erasure of redundant media prior to resale (remember to wipe the hard drive and memory in modern scanning copiers, etc.); physical security and audit trails (sign-out logs) for back-up media, policies about ownership and custodianship of data in partnership agreements and encrypted back-ups so when media is lost, included data is not disclosed. Similarly, proper physical and encryption protection of data on computing systems, training and processes with regard to storage of sensitive information in protected partitions, etc.; policies at major health institutions and within professional governing bodies to assist custodians in hard transitions (death or sudden departure of physician, etc.); proper system design, procedures and training to reduce external hacking threats. All of these things are cheaper and more effective than the events and consequences of the styles of privacy breaches listed above. (In some instances like outsourcing off-shore, very technical attention to contract terms and transport mechanisms, access and procedures of the vendor are required to mitigate potential breaches – but that is a whole other discussion, requiring a Privacy 401 discourse!)

Breach Situation "Checklist"

- Identify who in the organization is responsible for handling this matter.
- Identify the problem. What are the facts? Who is involved?
Which data is affected? What is the sensitivity of the data? How broad was the disclosure, and can it be contained somehow? Is the threat over, or is it continuing? What is the technical fix, going forward, both interim and longer term?
- Identify the parties at risk. Are patients at risk of some disclosure of their health or other personal information? Are caregivers at risk? Are referring agencies at risk?
- Determine the possible consequences of the breach. Is there a risk of identity theft? Is there a security risk (physical safety, access to other assets)? Is there a reputational or public health risk (communicable disease, AIDS, SARS, lifestyle, mental health, attributable statements for patients; prescribing habits, statements in files, financial data, etc. of clinic or care-givers)? Is there any other risk such as risk of losing patients' trust in clinic or physician?
- Determine how the risks can be identified, contained, minimized. Can the custodian/responsible organization provide assistance to those who have been placed at increased risk by the breach? Is there any public statement or notice which could be made or sent out to reduce fear, increase or maintain trust, or provide those affected with means to protect themselves or mitigate their own risk or consequences of breach?
- Identify legislated and contractual requirements to report the breach. Any professional obligations? Any contractual requirements?
- Determine who should be enlisted in assisting, repairing, containing, compensating, and dealing with the risks associated with the breach. Vendors, insurers, consultants, experts, security advisors, credit-reporting agencies, affiliated caregivers, privacy commissioner(s), others?
- Design a strategy for disclosure to those concerned. Will those concerned find out from you, from the newspaper, from someone else? How will those responsible handle the press, the authorities, the patients, and the staff?
- Focus on immediate next steps.

When dealing with a breach event (or circumstance), the responsible person (usually the system or office/ clinic administrator) has some heavy and immediate responsibilities. We suggest that a prudent approach to a breach situation should, at a minimum, include the steps indicated in the sidebar (each of which will require more or less thorough analysis depending upon the event).

Having set the stage, we now proceed to answer frequently asked questions.

Q1: What types of privacy breaches do you each see in your respective roles?

A1: Michael - We have been retained to assist in most of the situations above, either for the custodian or a vendor or consultant to the custodian. The breach is typically reported by an employee who either noticed the breach or accidentally perpetrated the breach, and came to management. It is very rare that a “data subject” will be the “first to know” about a breach. In some instances, we have done “what if” analyses of various breach scenarios, either in procedure and policy design (for caregiver organizations) or in system design and provisioning contracting (for vendors and consultants).

A1: LeRoy - We learn about a privacy breach either from the individual who has been affected, from the health service provider who decided to self-report a breach to the Commissioner or from the media. The types of breaches we investigate include improper disposal of records (electronic and paper), computer theft, unauthorized access to an electronic health record by an authorized user; generally any improper collection, use, access, disclosure or disposal of health information. It has been interesting to see that most breaches investigated have more to do with human error or poor judgment than the technical or security failings of a large information system. Breaches are normally caused by people making mistakes, or not following established policies or best practices, not by hacking.

Q2: What initial steps should be taken by an organization in responding to a privacy or security breach?

A2: Michael - the initial step SHOULD be to “refer to the PIA policy and procedures manual, which will have a detailed description of how to deal with a security or privacy breach”. In most cases, those policies are either silent or very superficial in providing guidance. To paraphrase the more detailed steps set out above, the first step is always to identify who is in charge and to find out as much as possible about the breach, its severity and nature, which systems are affected, and which persons are exposed to increased risk; the second step is to design the immediate response (which might be “shut it down” or “lock it down”, depending upon how “mission critical” the systems are) and assign responsibility for tasks to a very small number of people. Then, the real work begins: detailed risk analysis with respect to risk to the organization, risk to the entities involved, system repair, and risk mitigation. Risk mitigation includes analyses of who is better positioned to reduce risk and repair or reduce eventual harm, how to notify them, who to notify, who to involve.

Then the mind turns to cost-recovery (whose fault? Can they be made to pay or reimburse?) ... Oh, I forgot... you should of course also call your friendly privacy lawyer at an early stage!

A2: LeRoy - The most important step, which is easily overlooked, is the one taken before the breach occurs. You cannot effectively and efficiently respond to a breach without a plan and process that was previously accepted by the various health service providers in the organization. Those involved need a playbook to guide their steps – an incident response policy that says who will take leadership and provide direction for responding to the breach. Information about the breach must be quickly gathered and an initial assessment of risk completed. The initial assessment of risk should consider:

- The nature of information or data elements that have been breached
- The scope of the information exposure and whether there is ongoing risk of further exposure
- How to stem the breach

Once the extent of the breach is known and the initial risk has been mitigated, the incident response should shift to consideration of the cause of the breach and measures that could reasonably ensure it does not happen again. This should include:

- Review of administrative, technical and physical safeguards to determine whether they were effectively implemented and to identify any additional safeguards that would mitigate risk
- Internal and external communication
- Privacy and security training

Q3: Should the breach be reported to the authorities? Who are they?

A3: Michael - This we leave to our client, but typically we advise that it depends upon a number of things, including: how widespread is the problem, is it likely to be reported by others (or has it already been reported), for instance, police or credit card processors, insurance payors, patients or the press; is there any increase to the harm by reporting? Is there any harm from failing to report?

In most cases, we find that self-reporting has very few risks and tends to enlist the assistance (rather than the wrath) of the privacy commissioner’s office. If an investigation follows, having started on a co-operative footing, the investigation tends to go more smoothly and collaboratively (and not adversarially). Remember, the “authorities” may include professional governing bodies or regulatory bodies other than a Privacy Commissioner (the police, for example).

A3: LeRoy - We recommend reporting, but this depends somewhat on the extent of the breach and the organization's ability to investigate and appropriately respond independently. Reporting to the Privacy Commissioner's Office provides an opportunity for dialogue and to cooperatively address the various issues that arise. This does not necessarily mean that the matter will be dealt with publicly. We frequently receive self-reports and work with the health service provider to address the breach confidentially. Self-reporting demonstrates openness and accountability and provides a level of assurance to affected individuals. When a breach does become public, having already reported to the Privacy Commissioner helps avoid the perception that the matter was covered up. There should also be consideration of any obligation to report to a college or professional association, or whether there may be a contractual obligation to report.

Q4: Should the affected data-subject be notified? Who are they? How?

A4: Michael - in most cases, depending upon the severity of the effects of the breach on a data subject, there is a very strong case for notification of the facts and provision of information and sometimes remedial assistance, to the data-subject of leaked information or breached privacy. This seems to be a trend in privacy law, and also seems like "the right thing to do". In most cases, the data-subject will eventually find out about the increased risk exposure resulting from the breach, so early and complete notification in a helpful fashion will, from a legalistic and purely self-serving perspective, provide the wronged party with enough information to exercise their own efforts at mitigating those risk exposures and thereby limiting their eventual claim against the data custodian or data repository. In addition, in most (but not necessarily all) cases, full disclosure has an effect of regaining or restoring the data-subject's trust in the custodian and its systems. The question bears some further analysis, since notification can be more or less fulsome, more or less public, and contain more or fewer concessions and assistance, and so should be designed fairly carefully to ensure the best outcome, given the nature of the breach, its repair, its likelihood of recurrence, and its likelihood of causing harm to the data subject.

A4: LeRoy - It seems that notifying individuals affected by a privacy breach is becoming best practice and we are seeing a trend to require notification by law in some US states. Notification must be considered when a breach has occurred, however I do not believe notification is required in every case. An individual should be advised when something has gone wrong that could affect

them and be told what action can be taken to protect themselves, but this should be based on an assessment of harm. Where there is no reasonable risk of harm, there is no point to the notice. For example, there is much greater reason to provide notice of a data back-up tape that has been lost that is not password protected and encrypted than one where the information has been properly protected. A health service provider should assess the risk of harm and provide notice to all affected individuals when harm is reasonably foreseen. Notice can be provided directly or indirectly (i.e. via public announcement or advertising) and should include information about what can be done by the individual to protect him or herself. Considerations about when, how and what to include in a notice should be discussed with the Privacy Commissioner's Office and/or other authorities who can advise on the content of the notice, protective steps that can be taken and a plan for responding to questions from the individuals effected.

Conclusion

A breach of privacy can take many forms and may involve paper records, electronic records or both. Health information can be improperly disposed, wireless data can be intercepted, an electronic health record can be hacked or inappropriately accessed by an authorized user or improperly collected, used or disclosed.

Sometimes things go wrong and a privacy breach will need to be addressed. A health service provider is obligated to ensure reasonable safeguards are in place to protect health information. However, because it is not possible to foresee everything that can go wrong, it can be difficult to ensure the right safeguards are in place. Even then, industry best practice safeguards will reduce risk, but not eliminate human error. The obligation of a health service provider is not to guarantee that nothing will go wrong, but, through due diligence, to assess where risk lies and to implement reasonable measures to mitigate that risk.

When a privacy breach does occur, it of course needs to be remedied and its consequences dealt with. The key response objectives are to stem the breach and mitigate the immediate risk, and to take steps to reasonably ensure that it does not happen again.

While some privacy breaches simply cannot be foreseen, our experience shows us that many problems could have been avoided with better threat and risk assessment. The clinic that lost a data back-up tape ... if only it had been encrypted. The computer that was re-sold... if only the transcriptionist had not saved health information onto the hard drive or had wiped the drive. The clinic that was broken into ... if only the server holding health information was kept in a locked room.

A privacy impact assessment (PIA) is an effective front-end tool to examine these risks and identify the appropriate administrative, technical and physical safeguards to mitigate them. It guides a due diligence exercise where the health service provider examines the measures that are necessary to protect its information holdings. A PIA should be conducted for each system or project implemented that involves health or personal information. Completion of a PIA and implementation of the safeguards needed to reasonably mitigate risk is

preventive medicine that will help ensure there is no privacy breach, or if one occurs, that the response is well understood.

The best response to a privacy breach is the planned but unused response where a breach does not occur because foreseeable risk was mitigated.

In privacy, a good defense is better than a good offence. ●

***Michael Whitt** is a partner, lawyer, patent and trademark agent with the Borden Ladner Gervais law firm, and is a leader within the firm's Privacy Law, Information Technology, and Intellectual Property and Technology groups. He has had extensive experience in the healthcare informatics realm.*

*e-Mail: mwhitt@blgcanada.com
Telephone: 403.232.9751*

***LeRoy Brower** is Director, Health Information Act, Office of the Information and Privacy Commissioner, Alberta, and is responsible for leading a team the members of which oversee health service providers' compliance with the Health Information Act (Alberta). The team investigates privacy and security breaches involving health information, reviews and comments on privacy impact assessments about practices or systems involving health information and mediates disputes regarding access to health information.*

*e-Mail: lbrower@oipc.ab.ca
Telephone: 780.422.6860*