Complying with the Personal Health Information Protection Act

Debra Grant Ph.D.

Information and Privacy Commissioner/Ontario

Ontario Association of
Medical Radiation Technologists (OAMRT)
Owen Sound, Ontario
May 7, 2006

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature
- Widely shared among a range of health care providers for the benefit of the individual
- Widely used and disclosed for secondary purposes that are seen to be in the public interest (e.g., research, planning, fraud investigation, quality assurance)

Health Privacy is Critical

- The need for privacy has never been greater:
  - Extreme sensitivity of personal health information
  - Increasing electronic exchanges of health information
  - Multiple providers involved in health care of an individual – need to integrate services
  - Development of health networks
  - Growing emphasis on improved use of technology, including electronic patient records
  - Need to have a consistent set of rules across the health sector for these initiatives to move forward – privacy is key to successful reform


SEATTLE POST-INTELLIGENCER
GREENBERG
INSURANCE COMPANIES
EMPLOYERS
FINANCIAL INSTITUTIONS
MARKETERS

Privacy Risks: Unauthorized Disclosures

3rd Party Disclosures not authorized by patient may threaten integrity of system

- Fear of stigmatization, discrimination, loss of employment opportunities, denial of insurance, denial of housing

California HealthCare Foundation survey:

- One in six people engage in privacy protective behaviour to shield themselves from misuse of their information

Shielding Behaviours

- Multiple doctoring
- Out of pocket payments
- Avoiding testing
- Avoiding treatment
- Lying or withholding information from providers
- Asking providers to misrepresent diagnosis

Canadian Survey

- similar behaviors have been reported in Canada
- an EKOS survey estimated that 1.2 million Canadians have withheld information from a health care provider because of concerns over who the information might be shared with, or how it might be used
- an estimated 735 thousand Canadians decided not to see a health care provider for the same reasons
- lack of honesty and behavior change can reduce the accuracy of health data, with potentially undesirable consequences for patients, health care providers, government, and researchers

Organizational Risks

- **Privacy breaches:**
  - damage to an organization's image; loss of trust
  - Threat of privacy complaint and/or law suits
  - financial costs – damage control is often more costly than preventative measures
  - unwanted scrutiny from media, consumers and privacy advocates
- **Shielding behaviour:**
  - diminishes data quality and integrity

Is PHIPA a good thing?

Without PHIPA:

- Patchwork of rules across health sector
  - barrier to integration of services from multiple health care providers
  - barrier to implementation of new technology such as health infoways and EHRs
- Parts of health sector subject to PIPEDA and parts unregulated
- Duties of custodians and individuals' rights not clearly defined

What PIPEDA Wrought

- As of January 1, 2004, HICs in private practice covered by PIPEDA
- PIPEDA is a comparatively blunt instrument
- PHIPA drafted with the needs of the health sector in mind

Why is PHIPA a good thing?

- Provides a consistent set of rules for the collection, use and disclosure of personal health information across the health care sector
- Obligations of custodians and rights of individuals are clearly defined
- Because PHIPA is substantially similar to PIPEDA, custodians are exempt from the application of the federal rules
- In the event of a conflict PHIPA prevails over other legislation

What remains the same?

Many things remain essentially the same, with some variations in the details. Some examples are:

- The obligation to safeguard personal health information (PHI);
- The obligation not to disclose PHI except in limited circumstances or on consent;
- The ability to disclose PHI to reduce risk of serious harm;
- The obligation to provide access to PHI.

Does it strike the right balance?

- Designed to allow personal health information to flow among health care providers, but at the same time protect the privacy of individuals
- In the health care context, consent can be implied for the collection, use and disclosure of personal health information
- Outside the health care context, express consent usually required

PHIPA implementation

- Only 6 months from the time the legislation was passed until it came into force;
- Nonetheless, implementation was a surprisingly smooth process – it is business as usual in the heath care sector
- Custodians have done an excellent job, with a high level of cooperation with IPC in resolving issues;
- Relatively few complaints to the IPC – most complaints are being handled effectively by the custodians themselves.

Is it an undue burden on custodians?

New obligations

- Requires much more transparency –written statement of information practices available to the public; posting of notices when implying consent, etc.
- Appointment of contact person
- Privacy training and education
- Responding to lock box requests
- Individuals must be notified when security breached
- Dealing with an oversight body

How does PHIPA alleviate burden on custodians?

- Clearly no requirement for express consent in the context of providing care – not the case under PIPEDA
- Specified custodians may assume implied consent when providing health care
- Custodians only have to be concerned about one set of privacy rules – substantially similar designation
- Provides clear authority to collect, use and disclose personal health information without consent in a range of appropriate circumstances
- PHIPA is consistent with most existing standards of practice
- Variety of tools being developed by the IPC to assist custodians with implementation

Privacy Defined

- **Information Privacy: Data Protection**
  - Freedom of choice; control
  - Informational self-determination
  - Personal control over the collection, use and disclosure of any recorded information about an identifiable individual

The Foundation: Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

CSA *Model Code for the Protection of Personal Information*

Personal Health Information Protection Act (PHIPA)

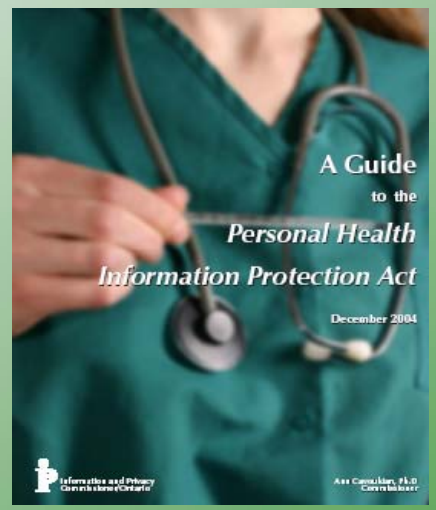
- Came into force November 1, 2004;
- Applies to organizations and individuals involved in the delivery of health care services (including the Ministry of Health and Long-Term Care);
- The only health sector specific privacy legislation in Canada based on consent: implied consent within the "circle of care," otherwise, express consent;
- The only health sector privacy legislation that has been declared substantially similar to the federal legislation.

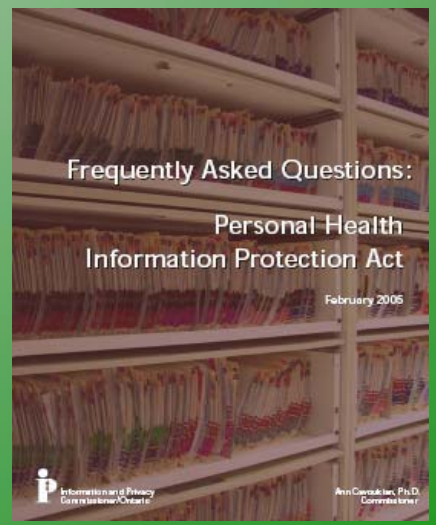
Mandate of the Legislation

- Require consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Require that health information custodians treat all PHI as confidential and keep it secure;
- Codify an individual's right to access and request correction of his/her own PHI;
- Give a patient the right to instruct health information custodians not to share any part of his/her PHI with other health care providers;
- Establish clear rules for the use and disclosure of personal health information for secondary purposes including fundraising, marketing and research;
- Ensure accountability by granting an individual the right to complain to the IPC about the practices of a health information custodian; and
- Establish remedies for breaches of the legislation.

Public Education Program

- Frequently Asked Questions and Answers
- User Guide for Health Information Custodians
- IPC PHIPA publications distributed to Colleges and Associations of the Regulated Health Professions;
- IPC/MOH brochure for the general public:
- OHA Toolkit





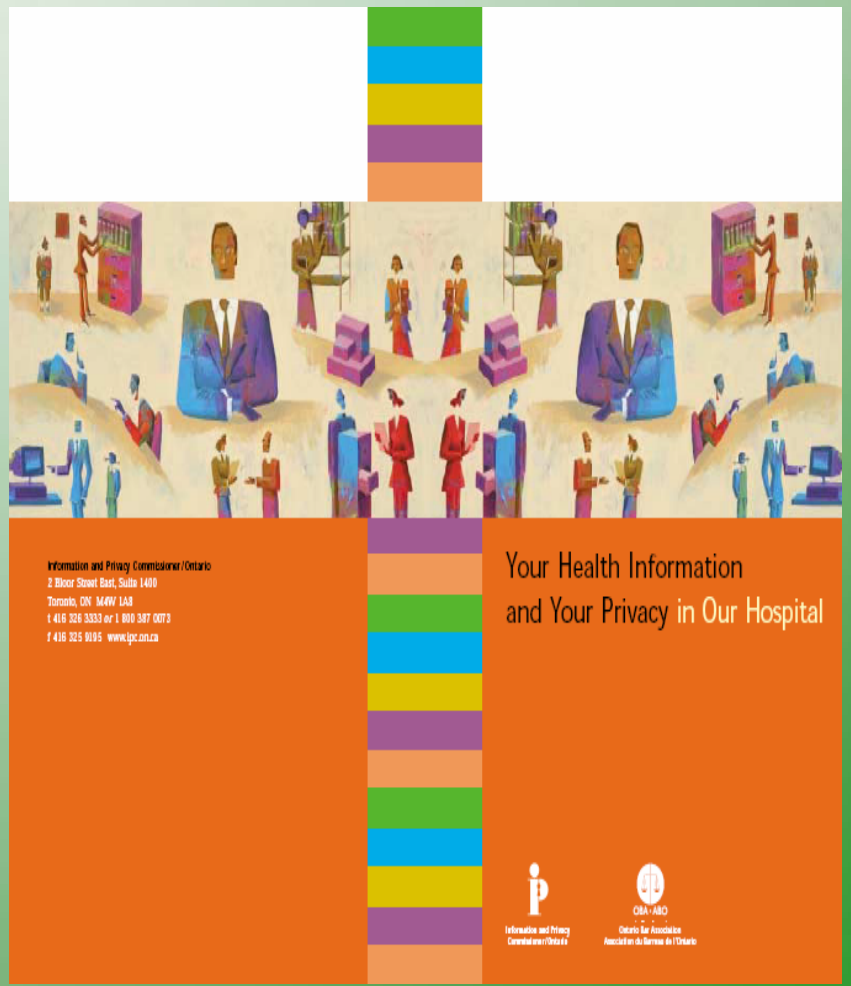
PHIPA: Fact Sheets

- Lockbox;
- Disclosure of Information Permitted in Emergency or other Urgent Circumstances;
- Reporting Requests under *PHIPA;*
- Consent and Form 14;
- Fundraising under *PHIPA;*
- Ontario Regional Poison Information Centres and the Circle of Care;
- Your Health Information: Your Access and Correction Rights;
- Safeguarding Personal Health Information.

Health Information Short Notices

- Goal was to develop easy to read products containing essential information about the collection, use and disclosure of personal health information, but not to overwhelm individuals with so much information that they will **not** read them
- Plain language is key
- Working group: IPC; Ontario Bar Association's Privacy and Health Law sections; Ministry of Health and Long-Term Care; Ontario Dental Association;

Short Notices Products



Privacy Impact Assessments (PIAs)

- Self-assessment tool developed to assist health information custodians in reviewing the impact of a proposed information system, technology or program on privacy
- Goal is to identify and mitigate privacy risks
- PIAs are not required under PHIPA, but are rapidly becoming a best privacy practice

Other Resources

- PHIPA Training Video – available upon request

Scope of PHIPA

- Applies to personal health information that is collected, used or disclosed by health information custodians
- Applies to personal health information that is received from a health information custodian (general rules/special rules for researchers, prescribed entities, prescribed registries, prescribed health data institute)

Health Information Custodians

- Definition includes:
  - Health care practitioner
  - Hospitals and independent health facilities
  - Homes for the aged and nursing homes
  - Pharmacies
  - Laboratories
  - Home for special care
  - A centre, program or service for community health or mental health

Complying with PHIPA

- First step is to determine your status under PHIPA – health information custodian; agent of custodian; provider; recipient
- Health care practitioners are considered to be custodians, except if they are agents of a health information custodian
- Agent defined as any person who acts for or on behalf of a custodian for the purposes of the custodian and not the agent's own purposes

General Rules for Custodians

- Most of the rules in PHIPA apply to custodians
- Must take reasonable steps to ensure accuracy and security of personal health information
- Must have a contact person to ensure compliance with the legislation and to respond to access/correction requests, inquiries and complaints from public
- Must have written information practices that comply with PHIPA and are available to the public
- Must obtain consent before PHI is collected, used or disclosed, unless permitted without consent
- Must be responsible for actions of agents – train and educate all staff on privacy and security

General Rules for Agents

- Only permitted to collect, use, disclose, retain or dispose of PHI on custodian's behalf if
  - the custodian is permitted to do so, and
  - it is in the course of the agent's duties
- Must notify the custodian at the first reasonable opportunity if PHI is stolen, lost or accessed by unauthorized persons
- Must comply with custodians information policies and practices

Consent Requirement

- A health information custodian shall not collect, use, or disclose personal health information unless:
  - Consent has been obtained and, to the best of the health information custodian's knowledge, the collection, use or disclosure is necessary for a lawful purpose; OR
  - It is permitted or required by the Act
- Consent may be express or implied, except when the Act specifies that consent must be express
- Consent, whether express or implied, must satisfy the requirements of the Act

(Sections 18 and 29)

Requirements for Valid Consent

Consent, whether express or implied, must:

1. Be the consent of the individual
2. Be knowledgeable, meaning it must be reasonable to believe that the individual knows:
   - The purpose of the collection, use or disclosure; and
   - That the individual may give or withhold consent
3. Relate to the information, and
4. Not be obtained by deception or coercion.

(Section 18(1))

Knowledgeable Consent

- It is reasonable to believe that an individual knows the purpose if the custodian posts or makes readily available a notice in a place where it is likely to come to the individual's attention

Express Versus Implied Consent

- Consent may be express or implied, except when the Act specifies that consent must be express
- Express consent is required:
  - To disclose personal health information to a non-health information custodian (subject to exceptions)
  - To disclose personal health information to another health information custodian for a purpose other than health care
  - To collect, use or disclose personal health information for marketing or market research
  - To collect, use or disclose personal health information for fundraising if use more than name and address

(Section 18(3), 32 and 33)

Assumed Implied Consent

GENERAL RULE

Some health information custodians whose core function is the provision of health care may assume implied consent to the collection, use or disclosure of personal health information for the purpose of providing or assisting in providing health care if the health information custodian receives the information from another health information custodian, the individual or the individual's substitute decision maker

EXCEPTION

If the health information custodian is aware that the individual has withheld or withdrawn consent

(Section 20(2))

Collection, Use and Disclosure

- Custodians may collect, use and disclose personal health information if:
  - The individual consents, or
  - The Act permits or requires the collection, use and disclosure

section 29

Indirect Collection Without Consent

- the information is necessary for the provision of health care and direct collection is not **reasonably** possible;
- custodian is a government institution and the information is needed for an investigation, proceeding or statutory function of the custodian;
- custodian collects the information from a person who is not a custodian for research purposes;
- custodian collects the information from a person who is not a custodian for planning and management of the health system (only applies to custodians prescribed by regulation);
- the Commissioner authorizes the indirect collection;
- custodian collects the information from a person who is permitted or required by law to disclose it; or
- where the collection is specifically permitted by law.

Permitted Uses Without Consent

- for the purpose for which it was collected or created;
- for a purpose for which it was disclose it to the custodian;
- for planning or delivering programs or services;
- for the purposes of risk management, error management or improving the quality of care;
- for educating agents who provide health care;
- for the purpose of disposing of the information or modifying the information to conceal the identity of the individual;
- for the purpose of seeking the individual's consent;
- for the purpose of a proceeding;
- for the purpose of obtaining payment for health care or related goods and services;
- for the purpose of research, subject to certain conditions; or
- if permitted or required by law.

Permitted Disclosures Without Consent

- disclosures relating to providing health care;
- disclosures by a facility that provides health care;
- disclosures relating to a deceased individual;
- disclosures for health or other programs;
- disclosures related to risks;
- disclosures related to care and custody;
- disclosures for proceedings;
- disclosures to a successor;
- disclosures related to this or other Acts;
- disclosures for research;
- disclosures for planning and management of health system;
- disclosures for monitoring of health care payments;
- disclosures for analysis of the health system; and
- disclosures with the Commissioner's approval.

Right of Access and Correction

PHIPA Expands and Codifies the Common-Law Right of Access

- Right of access to all records of personal health information about the individual in the custody or control of any health information custodian (some exceptions)
- Provides right to correct their records of personal health information (some exceptions)

Access/Correction Requirements

- Custodian must respond to requests within 30 days
- Custodian must provide access or copy
- Custodian must correct records that are inaccurate or attach statement of disagreement to the record if requested
- Upon request, custodian must notify recipients of any correction or statement of disagreement attached to record

Exclusions from Right of Access

- Access provisions do not apply to:
  - Quality of care information
  - Quality assurance program information
  - Raw data from standardized psychological tests
  - Other prescribed information
- Personal health information that is in the custody or control of a laboratory if:
  - The individual has a right of access through the health care practitioner;
  - The health care practitioner has not directed the laboratory to provide the information directly

Exceptions to Right of Access

- Record subject to a legal privilege
- Another Act prohibits disclosure
- Information collected for proceeding
- Information collected for investigation
- There is a risk of harm to individual or another person
- Record is subject to one of several exemptions that apply to government records

Exceptions to the Right of Correction

- Custodian does not have to correct a record if:
  - It was not created by the custodian and the custodian does not have sufficient knowledge, expertise or authority to correct the record
  - It consists of a professional opinion or observation made in good faith

Security Requirement

- A health information custodian shall take steps that are **reasonable** in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copy, modification or disposal.

Section 12(1)

Implications of Security Requirements

- Privacy and security threats posed by new information and communication technology (cell phones, Blackberries, email etc.) must be assessed and minimized – conduct PIAs and TRAs
- Technology solutions must be accompanied by privacy and security policies and procedures

Oversight and Enforcement

- Office of the Information and Privacy Commissioner is the oversight body
- IPC may investigate where:
  - A complaint has been received
  - Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene the Act
- IPC has powers to enter and inspect premises, require access to PHI and compel testimony

Powers of the Commissioner

- After conducting an investigation, the Commissioner may issue an order
  - To provide access to, or correction of, personal health information
  - To cease collecting, using or disclosing personal health information in contravention of the Act
  - To dispose of records collected in contravention of the Act
  - To change, cease or implement an information practice

- Orders, other than for access or correction, may be appealed on questions of law

Role of IPC under PHIPA

- Use of mediation and alternate dispute resolution always stressed
- Order-making power used as a last resort
- Conducting public and stakeholder education programs: education is key
- Comment on an organization's information practices

Keeping HIC's Informed

- Orders will be public documents and available on our Web site
- Summaries of all mediated cases will be available on our website
- Relevant data will be regularly made available to the public and health professionals (*e.g. number of complaints, examples of successful mediations, common issues*)

As of March 15, 2006							
TOTAL PHIPA COMPLAINTS (OPEN+CLOSED)						**Total**	%
Access/Correction						102	40%
Collection/Use/Disclosure						69	27%
HIC Reported Breach						59	23%
IPC Initiated Complaint						26	10%
				Total		256	100%
OPEN PHIPA COMPLAINTS BY STAGE							
	Intake	**Mediation**	**Adjudication**			**Total**	%
Access/Correction	8	13	2			23	25%
Collection/Use/Disclosure	22	6	2			30	33%
HIC Reported Breach	13	0	11			24	26%
IPC Initiated Complaint	3	0	11			14	15%
				Total Open		91	100%
CLOSED PHIPA COMPLAINTS BY STAGE/METHOD CLOSED							
	Letter	**Letter**	**Report**	**No Order**	**Order**	**Total**	%
Access/Correction	60	18	0	1	0	79	48%
Collection/Use/Disclosure	32	7	0	0	0	39	24%
HIC Reported Breach	8	4	23	0	0	35	21%
IPC Initiated Complaint	6	0	5	0	1	12	7%
				Total Closed		165	100%

Has PHIPA achieved its Promise?

- Very few complaints – as of March 15 – only 256 files opened
- Only 102 complaints about access/correction
- Only 69 complaints about collection, use and disclosure
- 59 self-reported breaches by custodians
- 26 complaints initiated by IPC
- Only one order issued
- Most complaints resolved at an early stages through mediation

Film shoot uses real medical records

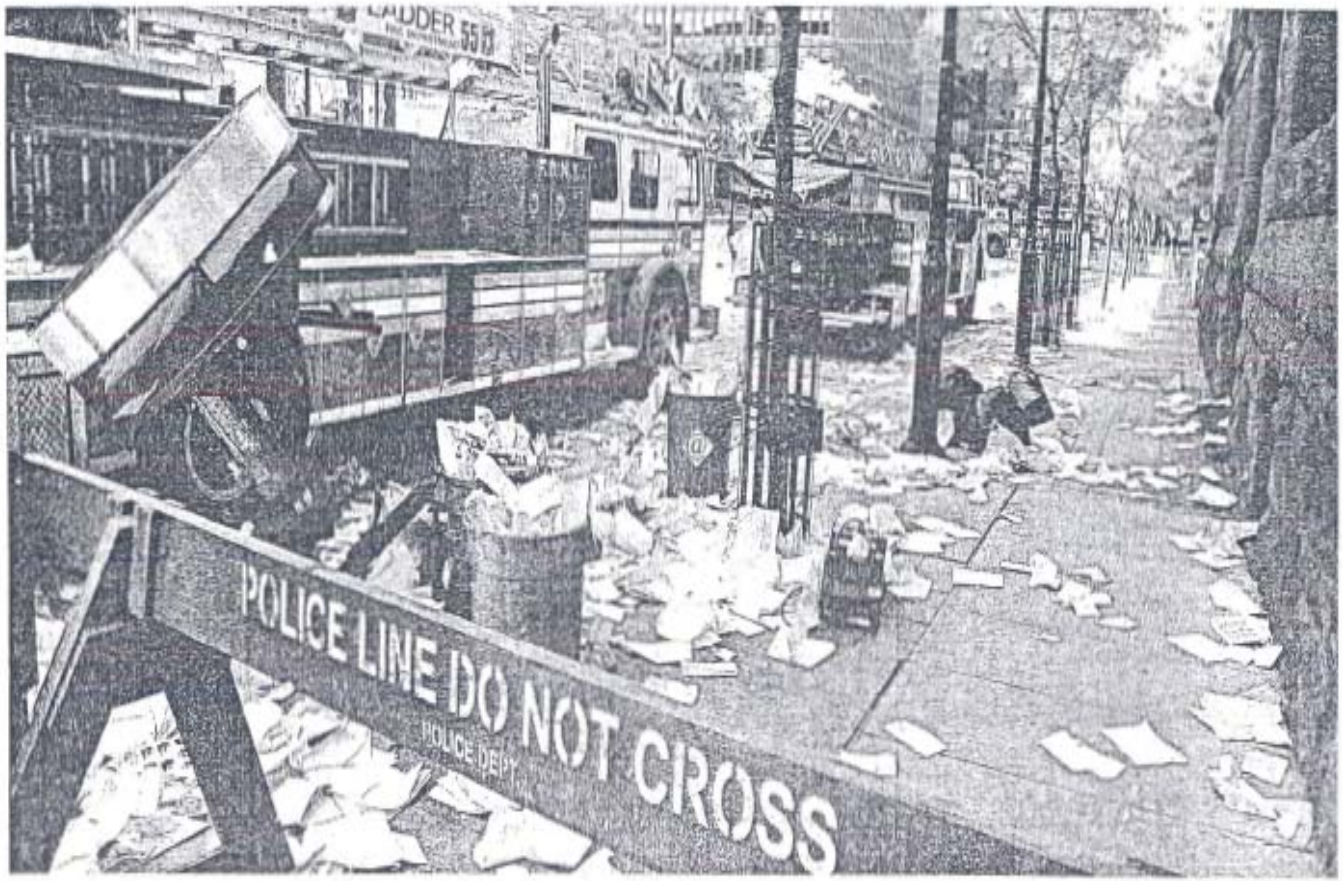
Privacy official has plans to investigate

RAJU MUDHAR
STAFF REPORTER

A TV miniseries filming in downtown Toronto may have to answer to Ontario's privacy commissioner after it was discovered that "fake garbage" used in the movie actually consisted of patients' medical records from a Bathurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untitled History Project*, a Touchstone Television production about the Sept. 11, 2001, terrorist attacks on the United States that will air on ABC. Toronto is filling in for New York City, and fire trucks, police cruisers and strewn garbage are being used to recreate the scene.

But much of the garbage yesterday was actually medical documents – mostly information about X-rays bearing the address of a Bathurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even diagnos-



TONY ROCK/TORONTO STAR

Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

Ongoing implementation issues

- Fees
- Lock box
- Notification of Security Breaches
- Electronic Health Records

Fees

- IPC has had many complaints and inquiries about fees for access to records of phi – no consistency in interpreting what is “reasonable cost recovery” hence costs vary widely from one custodian to another
- Proposed regulation will address this issue – custodians would be able to charge a base fee of $30 that would cover most access requests
- The IPC lobbied for and welcomed the fee regulation
- Many different stakeholders had their say

Lock Box

- Where the individual expressly withholds or withdraws consent or instructs a custodian not to use or disclose personal health information without consent for the purpose of providing health care
- Withdrawal of consent critical for substantial similarity designation
- Hospitals face ongoing challenges in incorporating lock box functions into existing health information systems
- Legacy systems were not designed to accommodate consent preferences
- Some systems capable of locking information at the encounter or record level
- Required level of granularity is an issue – PHPA does not put any limits on what the individual may request in terms of locking

Checks on the Lock Box

- **Notification** – if a custodian who discloses, without consent, believes that all information necessary for the the provision of health care has not been disclosed, the custodian must notify the recipient *Section 38(2)* – proposed regulation will also require notification of agents within a health information custodian
- **Override** – custodian may disclose (regardless of individual's wishes) if necessary to eliminate or reduce a significant risk of serious bodily harm to a person or a group of persons *Section 40*

Further Limits on the Lock Box

- **Documentation** – Conditions placed on and individual's consent cannot prohibit the recording of information that is required by law, established professional practice, or institutional practice

Section 19(2)

IPC Position on Lock Box

- Lock box provisions came into full force as of November 1, 2005;
- Fact sheet available on IPC website;
- IPC does not expect custodians to invest in expensive technological solutions to implement the lock box, that may only be requested by a small number of patients;
- IPC expects custodians to develop creative solutions to respond to individual requests;
- Manual solutions to address the need for a lock box are quite acceptable.

Notification

- Section 12(1) requires custodians to notify the individual at the first reasonable opportunity if personal health information is stolen, lost or access by unauthorized persons

Notification Challenges

- Sometimes the identities of individuals are not known (e.g., no backup for lost laptop)
- Sometimes there are a large number of individuals involved and individual notification may not be practical or possible
- Sometimes it is not known what has happened to the information (e.g., custodian doesn't know if there was any unauthorized use or disclosure of lost information) so custodian may not know what to tell the individual about the breach
- Notification may cause unnecessary stress for individuals who may already be facing life threatening illness

Notification Solutions

- IPC is working with custodians to develop creative solutions to notification requirement
- Posting general notices in newspapers, physician's offices, health care facilities and other places where it is likely to come to the attention of affected individuals
- Notification in person at next scheduled appointment rather than by letter

Emerging Medical Radiation Technology

- Move from analogue to digital imaging has both benefits and risks
- Digital images do not deteriorate; easier to store and manipulate
- Digital images can be shared electronically
- Digital images are one type of electronic health record – has some of the same advantages and challenges as any other EHR

Digital Imaging

- Digital imaging is considered to be a key building block for the EHR by CHI – substantial funding investment
- Digital imaging systems enable health care providers to view, manage, distribute and electronically store patients' test images, MRIs, X-rays, CT scans, PET scans, and medical files from any location connected to the system
- The PACS (picture archiving and communication system) captures, stores and sends images using digital technology

Digital Imaging Pilots Funded By CHI

Diagnostic Imaging - ON Thames Valley Hospitals
Diagnostic Imaging - Ontario - TEN Group
Diagnostic Imaging - Pan Northern Ontario
Diagnostic Imaging - Southwestern Ontario

Electronic Health Records (EHR)

Advantages

- Improve quality and lower cost of health care
- Quick access to wide range of data
- Better security through more effective access controls and audit trails
- Improve privacy protection by limiting access to those with a need-to-know (e.g., role based access)
- Better data for health system management, enhancing quality of care, and research

More about EHRs…

Challenges

- Facilitates data linkages and data sharing
- Unauthorized access is more catastrophic due to volume of records and quantity and quality of data
- Multiple users and multiple access points raises accountability issues and increase vulnerability

Some Key Questions

- Who retains custody and control of the shared archive of images?
- Who decides who has access to what information in the archive and under what circumstance?
- Who checks for privacy breaches?
- Under what legislative authority can a custodian transfer custody and control of the images to a central archive?
- What is the legal status of a central archive? (e.g., agent, custodian, registry, etc)

How to Contact Us

Debra Grant

Information & Privacy Commissioner/Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8

Phone: (416) 325-9170

Web: www.ipc.on.ca

E-mail: debra.grant@ipc.on.ca