Privacy and Security Training for Connecting Ontario

PACE Cardiology

April, 2017

Session Goals

By the end of this session you will:

- ✓Review key elements of privacy protection
- ✓Know your privacy obligations when using clinical systems
- ✓Know the added privacy obligations arising when clinical systems are "shared systems"

What's New in this Session?

Mainly, "shared systems" such as ConnectingOntario, which

- Combine patient information from several healthcare organizations
- Permit access only for providing care or assisting in provision of care—NOT for research, quality improvement, education or any other purpose
- May permit patients to block access to their information and
- May let you know a patient has blocked access and give you options for responding to the block

Basic Background

Privacy: the right to control access to information about oneself. Patients exercise this control by consenting to access for specific purposes.

PHI stands for Personal Health Information: practically any information related to the health or health care of an identifiable person.

PHIPA stands for the *Personal Health Information Protection Act, 2004*—the key law protecting PHI And patient privacy in Ontario.

Under the PHIPA privacy law

- PACE and its “Agents”—including you—must protect PHI and privacy.

- The two most important rules to know are these:
  1. **Access only PHI you need to know** to perform your PACE duties
  2. **Promptly report suspected privacy breaches** to the PACE privacy office

- A **privacy breach** occurs when PHI is lost, stolen or subject to unauthorized access, or when policies aimed at protecting privacy are violated.

- If you breach privacy, PACE and/or a professional college may discipline you.

Privacy Protection Matters

When you help protect privacy, you

- ✓Help ensure patient confidence in privacy protection, so that patients are willing to share all the information vital to their care
- ✓Honour the trust patients place in you and PACE Cardiology
- ✓Show respect for patients as individuals
- ✓Help protect your own reputation and PACE's
- ✓Avoid harm to patient and penalties for you and PACE
- ✓Meet legal, ethical and professional obligations

Breach Penalties are Increasing

- Organizations (including PACE) can now be fined up to **$500,000** for an offense under PHIPA, and individuals (including you) up to **$100,000**
- AND organizations can now face **lawsuits including class actions**, and individuals can face **civil litigation and prosecutions**
- AND increasing media attention and scrutiny by the Privacy Commissioner's office means increased **reputational risk** for PACE and for individuals.

Using Clinical Systems

"Clinical Systems" are computer systems used to support patient care (e.g., the PACE Cerebrum EMR, the ConnectingOntario system).

Important points about clinical systems:

- Practically anything you access through them is PHI, and therefore is subject to protection obligations
- They track which PHI you access, and when you access it
- Those responsible for these systems (e.g., PACE, eHealth Ontario) are obliged to audit user activity, to ensure that privacy rules are followed.

Using Clinical Systems

Important points (continued):

- Read carefully any “End User Agreement” or “I agree” statement you see when using these systems. They commit you to privacy-protective obligations.
- Commonly detected breaches include looking at the PHI of friends, relatives, neighbours, colleagues or celebrities.
- Unauthorized use of clinical systems will result in penalties. Violators are increasingly being caught and punished. Example:
  - “Ontario student fined $25,000 for accessing personal health info without permission” —*Globe and Mail*, March 16 , 2017

Using Clinical Systems

If you are ever in doubt about whether you may access PHI, consider this question:

“Do I need to access this PHI in performing my PACE-assigned duties, and if so, could I later explain that need?”

If the answer in either case is “No”, refrain from access.

If a patient has a question or complaint…

…about the protection of PHI or privacy, please:

1. let them know their issue is important to you and to PACE, and that you will address it—either directly, or through the PACE privacy office

2. address the issue if you can, or if not,

3. let them know that the privacy office (1-888-978-4701) will help.

If a patient asks for access to PHI…

1. Acknowledge their right to make the request and have it addressed.

2. If the request
   - is informal
   - can be met readily, without disrupting care and
   - is not subject to any unusual restrictions

   then fulfill it on the spot.

3. Otherwise refer the patient to the PACE privacy office (1-888-978-4701).

If a patient wants to restrict access to PHI

1. Acknowledge their right to make the request and have it addressed.
2. If you are a clinician, explain to the patient the clinical risks involved.
3. If they still wish to proceed, refer them to the PACE privacy office.

If a patient asks why access to some or all of their PHI has been blocked in a clinical system…

…promptly contact the PACE privacy office, which can get the PHI unblocked, if that is the patient's wish.

The PHI may have been blocked

- Inadvertently
- through a substitute-decision maker, or
- at a time the patient does not recall.

If a clinical system indicates a patient's PHI is blocked or restricted…

…read the blocking message carefully and then choose the correct response:

1. proceed without accessing the record, if you have no reason for access that is listed on the screen; or
2. choose a listed reason for access, and then proceed to the record. In this case, details of your access will be reported to the patient, in some systems.

To Protect PHI in Clinical Systems

- ✓Log into the system only with your own credentials
- ✓Never let others use your credentials
- ✓If you are leaving, log out or lock your device
- ✓If you must put PHI on a mobile device, use only an IT-approved encrypted device
- ✓If you must leave a device in a car, lock it in the trunk
- ✓Ensure unauthorized people cannot see your display screen

To Protect PHI in Clinical Systems (continued)

- ✓Don’t take pictures or screenshots of displays
- ✓Print only if the system has a Print button, and then print only what you need
- ✓If you must download PHI, download only what you need, and only to a secure location—e.g., a password-protected file on a PACE file server, or an IT-approved encrypted USB key.

To Protect PHI when Using Email

- ✓ Only send email from a PACE email address, or from an address on the secure eHealth Ontario network (e.g., a hospital address, or a ONE ID address) and
- ✓ Ensure all recipients have a PACE address or an address on the secure eHealth Ontario network.
- ✓ Before pressing Send, double-check recipient addresses.
- ✓ When you receive an email, unless you are sure it is from a trustworthy source, never click on a link or attachment, or respond with confidential information such your password.

Shared Systems…

- …are clinical systems combining PHI from multiple healthcare organizations. They may offer potential access to millions of records.
- Examples include ConnectingOntario, and hospital systems to which PACE users have been granted access
- When accessing a shared system as a PACE user, you are acting as PACE's "Agent" and are therefore accountable to PACE for your actions in using the system.
- All clinical-systems rules for protecting privacy apply as well to shared systems. But for shared systems, there is an ADDITIONAL rule.

The ADDITIONAL Rule, for Shared Systems:

You may ONLY access shared systems to provide care for, or assist in providing care for, your patients.

That is, shared systems are only available for clinical care and must not be used for any other purpose such as education, research, quality improvement or risk management.

Use of shared systems is vigorously audited by external parties. For example, eHealth Ontario audits how often users access particular patients, in order to catch people using ConnectingOntario for research.

In Summary

You are responsible for protecting the PHI you access through clinical systems, including shared systems.

You may ONLY access shared systems to provide care for, or assist in providing care for, your patients.