



UNIVERSITY OF OTTAWA
HEART INSTITUTE

INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Clinical Research Mandatory Training

Last updated: 29 Apr 2020



Introduction & Objectives

Introduction

This training is mandatory for all staff involved in clinical research.

Objectives

1. The learner should gain a better understanding of privacy as it relates to clinical research, specifically:
 - Governance of research privacy
 - Circle of care definition
 - Need for expressed consent before contacting for research purposes
 - Protection of data
 - Privacy breaches
2. The learner should gain an understanding of EPIC, the electronic health record (EHR) system used by the Institute, and the related privacy considerations.
3. The learner should gain an understanding of UOHI process and expectations for the Health Canada mandatory reporting of Serious Adverse Drug Reactions (SADR) and Medical Device Incidents (MDI)



UNIVERSITY OF OTTAWA
HEART INSTITUTE

INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Clinical Research Privacy Training



Privacy Definition

What is privacy?

The right for an individual to determine who knows what about him/her and what they do with the knowledge.



What legislation is in place to govern privacy in clinical research?

- **Personal Health Information Protection Act (PHIPA)**

- The law, developed in 2004, governs the way in which personal health information (PHI) can be accessed, collected, used and disclosed
- It ensures the right to access one's own PHI
- It is enforced by the Information and Privacy Commissioner's (IPC) Office of Ontario
- It is the responsibility of the Health Information Custodian (HIC) to protect the information
- Different rules apply for research purposes

- **Other governance in research privacy:**

- TCPS 2: The Tri-Council Policy Statement: Ethical Conduct
- ICH E6(R2) GCP Guidelines: International Council for Harmonisation Guideline for Good Clinical Practice



Privacy Policies

The University of Ottawa Heart Institute (UOHI) and The Ottawa Hospital (TOH) have a number of policies related to privacy, including but perhaps not limited to:

- UOHI Privacy 1-200 / TOH Privacy 00175
- Passwords, UOHI Policy 5-30
- Email Access & Usage, UOHI Policy 5-100
- Data Governance, UOHI Policy 5-140
- Corporate File Retention and Destruction, UOHI Policy 1-140
- Freedom of Information Requests, UOHI Policy 1-160
- Social Media, UOHI Policy 1-330

You should familiarize yourself with these policies which can be found posted on the [Heart Hub](#) (please note, this is the internal website only accessible from onsite).



OHIRC Privacy Policies & Other Governance

The Ottawa Heart Institute Research Corporation (OHIRC), the research arm of the UOHI, also has privacy policies, SOPs and other governance in place:

Policies

6-10 Responsible Conduct of Research

6-40 Research Involving Humans

6-90 Responsibilities of Principal Investigators

6-160 Data Security & Confidentiality for Clinical Research Databases

Clinical Research SOPs

C-1-002 Regulatory Requirements & Essential Documents

C-1-003 Privacy and Confidentiality

C-1-004 Team Roles & Responsibilities

C-1-005 Staff Training

C-1-009 Data Sharing Agreements

C-1-010 Management of Clinical Research Data

C-3-003 Master Subject List Requirements

C-3-004 Source Documentation



OHIRC Privacy Policies & Other Governance Con't

Research Ethics Board

Provides oversight by reviewing and approving the Privacy Plan submitted with the study application.

NOTE: REB approval of your plan to protect participant privacy and confidentiality is required by PHIPA – it's the law! (Explained in the coming slides) Any changes to the approved plan (screening a new clinic, promoting somewhere new, approaching through MyChart, etc.) must be approved by the REB *before* initiating or the actions could be considered a breach in privacy.

Security and Systems Access (SSA)

Ensures each new worker at UOHI reviews the expectations for privacy by obtaining a signature on the Acknowledgement and Confidentiality Agreement.



PHIPA & Research

PHIPA specifically addresses disclosure for research in Section 44:

- (1) A health information custodian (HIC) may disclose personal health information (PHI) about an individual to a researcher if the researcher,
 - (a) submits to the custodian (TOH/UOHI have delegated this responsibility to the Research Ethics Board (REB)):
 - (i) an application in writing,
 - (ii) a *research plan that meets the requirements of subsection (2), and
 - (iii) a copy of the decision of a REB that approves the research plan; and
 - (b) enters into the agreement required by subsection (5). [confidentiality agreement]

* (most commonly referred to as the “Privacy Plan”)



PHIPA & Research Con't - REB Considerations

In terms of the REB's role, Section 44 states:

- (3) When deciding whether to approve a research plan that a researcher submits to it, a REB shall consider the matters that it considers relevant, including,
- (a) whether the objectives of the research can reasonably be accomplished without using the PHI that is to be disclosed;
 - (b) whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose PHI is being disclosed and to preserve the confidentiality of the information;
 - (c) the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed; and
 - (d) whether obtaining the consent of the individuals whose PHI is being disclosed would be impractical.



PHIPA & Research Con't - Researcher Compliance

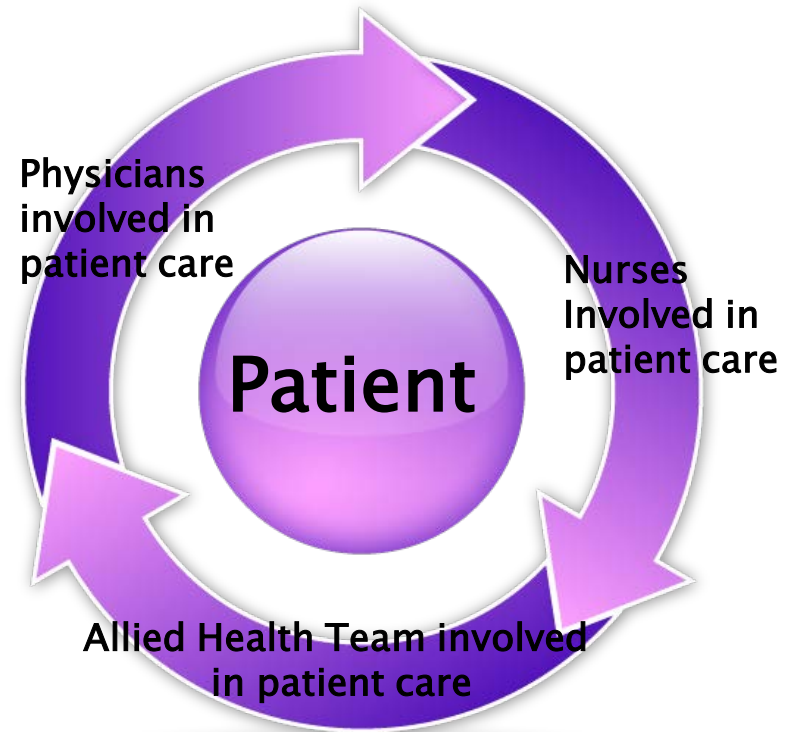
Under PHIPA the researcher [including the study team members] must be compliant as follows:

- (6) A researcher who receives PHI about an individual from a HIC under subsection (1) shall,
- (a) comply with the conditions, if any, specified by the research ethics board in respect of the research plan;
 - (b) use the information only for the purposes set out in the research plan as approved by the research ethics board;
 - (c) not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;
 - (d) despite subsection 49 (1), not disclose the information except as required by law and subject to the exceptions and additional requirements, if any, that are prescribed;
 - (e) not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual's consent to being contacted; (*Referred to as expressed consent, which is explained in the coming slides*)
 - (f) notify the custodian immediately in writing if the researcher becomes aware of any breach of this subsection or the agreement described in subsection (5); and
 - (g) comply with the agreement described in subsection (5).



Circle of Care

- This term is not defined in the PHIPA legislation, yet is used frequently in reference to research privacy and confidentiality.
- Only those who would normally have access to the patient's PII/PHI, and be in contact with the patient, for the purpose of providing health care are considered part of the "circle of care". This includes treating physicians, nurses, technicians, and registration clerks or administrative assistants managing patient testing or visits.
- Research staff are NOT considered part of the circle of care and **must not** approach or contact patients without their prior expressed consent documented with the HIC (in EPIC or a clinic chart).





Permission to Contact Process

To facilitate research, TOH and UOHI collaboratively developed a process to obtain a patient's permission to be contacted for research purposes.

Registration Clerks at outpatient units obtain permission by following an approved script:

What Do I Say to the Patient?

“As you probably know we do a lot of research here. If we have a study that may be appropriate for you, is it ok if our research staff contact you?”

If they agree right away, stop here and enter decision in Epic; if they hesitate or ask for more information, proceed with the following:

“Saying ‘yes’ means you may be contacted, but it doesn’t mean that you are agreeing to participate in research. It just allows our research staff to contact you to explain research studies that may apply to you.”

Either way, then follow with:

“Here is a FAQ sheet that provides more detailed information for you.” (Patient is provided a handout which includes contact information for the UOHI Privacy Officer)

There are three possible entries into Epic by the clerk:

“Yes”, “No”, “Undecided” (had the discussion but the patient was unable to decide or too overwhelmed to consider)



Permission to Contact Process Con't

- Once the patient provides his/her permission to be contacted (PTC) to the registration clerk, it is visible in real time in the header of the patient's EPIC medical record.
 - FYI: Using a pre-programmed smart text, any clinical staff may request an update to the patient's PTC status, in EPIC, should they obtain the patient's permission to be contacted (a Tip Sheet is available for them).
- The permission does not expire, however for respect of the patient, he/she will be asked again at their first visit after three years from the last permission.



Managing Research Data

- As previously explained, the HIC (TOH/UOHI) delegates the protection of patient privacy and confidentiality for research related activities to the Research Ethics Board (REB) (Ottawa Health Science Network Research Ethics Board (OHSN-REB) or a Board of Record through the Clinical Trials Ontario (CTO) Streamline Ethics System)
- Investigators must detail their *Privacy Plan* in the REB application, and obtain approval
- Research data leaving the HI should be de-identified / coded (strip the identifiers ASAP)
- Cardiac diagnostic images being sent off-site must be processed by the Cardiac Imaging Research Core Lab (CIRCL)
- Sharing data with external Investigators typically requires a Data Sharing Agreement or a Contract (even sharing between TOH and UOHI requires an agreement)
- Data collected at UOHI is the property of the Institute and must remain here, e.g.: may NOT be removed with trainee/fellow/researcher departure



Managing Research Data Con't

The Informed Consent Form (ICF) must disclose to study participants all plans for their PHI/PII

- What data will be accessed, used and disclosed
- Who will have access to the PHI
- How and where it will be stored – hard copies and electronic records
- What safeguards are in place for its protection
- What will be released to the Sponsor of the study and how it will be transferred
- How long the information will be saved and how it will be disposed/deleted



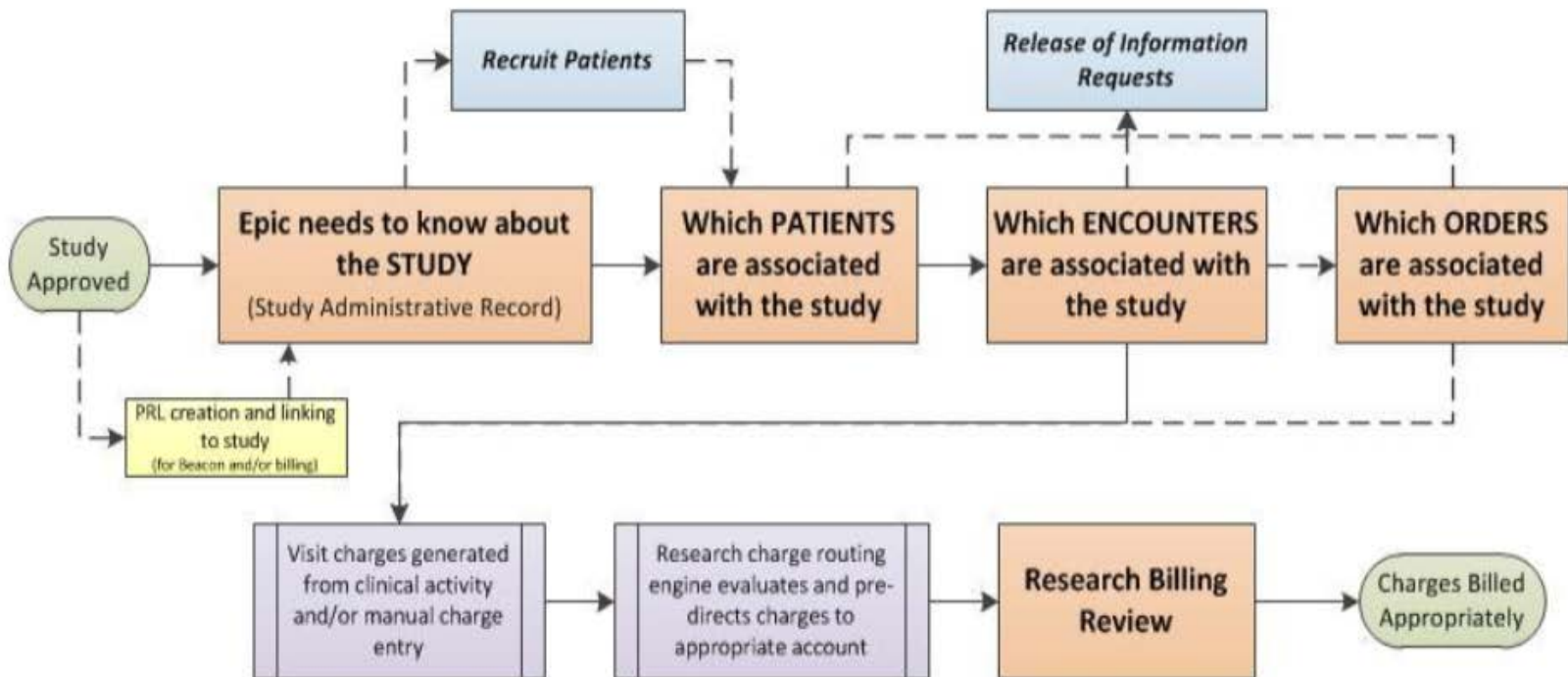
Introduction to Epic

- EPIC is the electronic health record (EHR) system for our patients, launched in June 2019.
 - Patient health information dating back 5-6 years was imported directly into EPIC, from the previous EHR system. Older records may be accessed through an “archive” link within the patient’s EPIC record.
- With the introduction of Epic, much of the clinical research management and documentation is now incorporated within the patient’s EHR.
- All research activities are documented in Epic, including all orders and visits associated with the study protocol.
- Research information for any patient enrolled in a clinical research study can be accessed by clicking on the *Research/Contact* link in the patient header of the chart.
 - This link will turn green only if the patient is enrolled in an interventional study.
- Research activities are also visible in the *Chart Review* section of the patient’s chart.



Introduction to Epic

Key Areas of Research Functionality





Access Levels in Epic

There are two levels of research access:

- “View/read-only”, for those collecting retrospective data (“secondary use of information”) from the chart, or
- “Coordinator” access for those managing prospective clinical research studies and documenting in the patients’ records.

Staff requiring Coordinator level access in Epic must complete classroom training prior to accessing patient records.

NOTE: Every “role” assigned within EPIC has a different view of the patient’s EHR, so just because you see something doesn’t mean someone else sees it in the same way or in the same location. Each role also has different security levels and abilities within EPIC.

Coordinators, for example, are not permitted to “create” new patient files; this is only available to a “registration clerk” role.



Break the Glass

- Break the Glass is a feature in EPIC which is used when patients wish to limit access to their health information.
- It appears when you try to open a patient's protected health record.
- If a patient has consented to research it does NOT mean that research staff can automatically break the glass in his/her EHR.
 - When you see a break the glass warning, you **must** contact the patient/study participant to ask permission to access their chart.
 - Only with his/her permission may you then break the glass.
 - Document his or her consent and the reason for breaking the glass in your records.
 - **NOTE:** This must be done EACH time you need to access the chart, unless they give you permission for the life of their participation in the study; which must be clearly documented in your records.

DO NOT BREAK THE GLASS UNDER ANY CIRCUMSTANCES for retrospective data collection studies (i.e. secondary use of information).



Security in Epic

Please remember these important security measures when using Epic:

- Be sure to logout when you are finished
- NEVER share your login and password
- Only access the information you require to complete your work

Additional Epic Information and Resources:

- The Clinical Research Compliance and Support pages on the Heart Hub, UOHI's internal website, offer many resources, including informative Tip Sheets on how to use functions or complete tasks within Epic.
- If you have any questions about accessing Epic or require more information, please contact clinicalresearch@ottawaheart.ca



Reminders for Protecting PHI

Physical Protections

- Locked offices with restricted access, locked filing cabinet
- Minimal hard copy records – do not print copies from EHR unless absolutely needed; the electronic version is the official record/source document
- PHI must be stored separately from de-identified, coded study/research records (e.g., signed consent forms, demographic pages, etc. must be separated from the case report forms)

Administrative Protections

- Limit access to only those who need it
- Governing Policies and Procedures as discussed earlier → compliance is assessed with monitoring and internal auditing practices

Technological Protections

- Store PHI only on hospital secure network drives – NEVER the C drive or a personal mobile device (only a UOHI encrypted device may be used, if mobile use is required, and only after permission has been explicitly granted by the REB as part of the privacy plan)
- Encryption and strong passwords



Email & Faxing

Email

- PHI can only be sent internally and to a secure (UOHI or TOH) email recipient that has a need to know
- Do NOT include PHI in subject line
- If identity must be shared, wherever possible use the MRN and initials rather than name
- If possible, have PHI in a separate password protected attachment – and provide password in a separate email or by phone
- ALWAYS verify the “To” field before sending

Faxing

- Use a formal fax cover letter if the fax is going to an external fax machine
- ALWAYS verify the fax number before sending
- If you are expecting a fax containing PHI, wait by the fax machine to receive it
- ** Considered safer than email by the Office of the IPC of Ontario



What is a privacy breach?

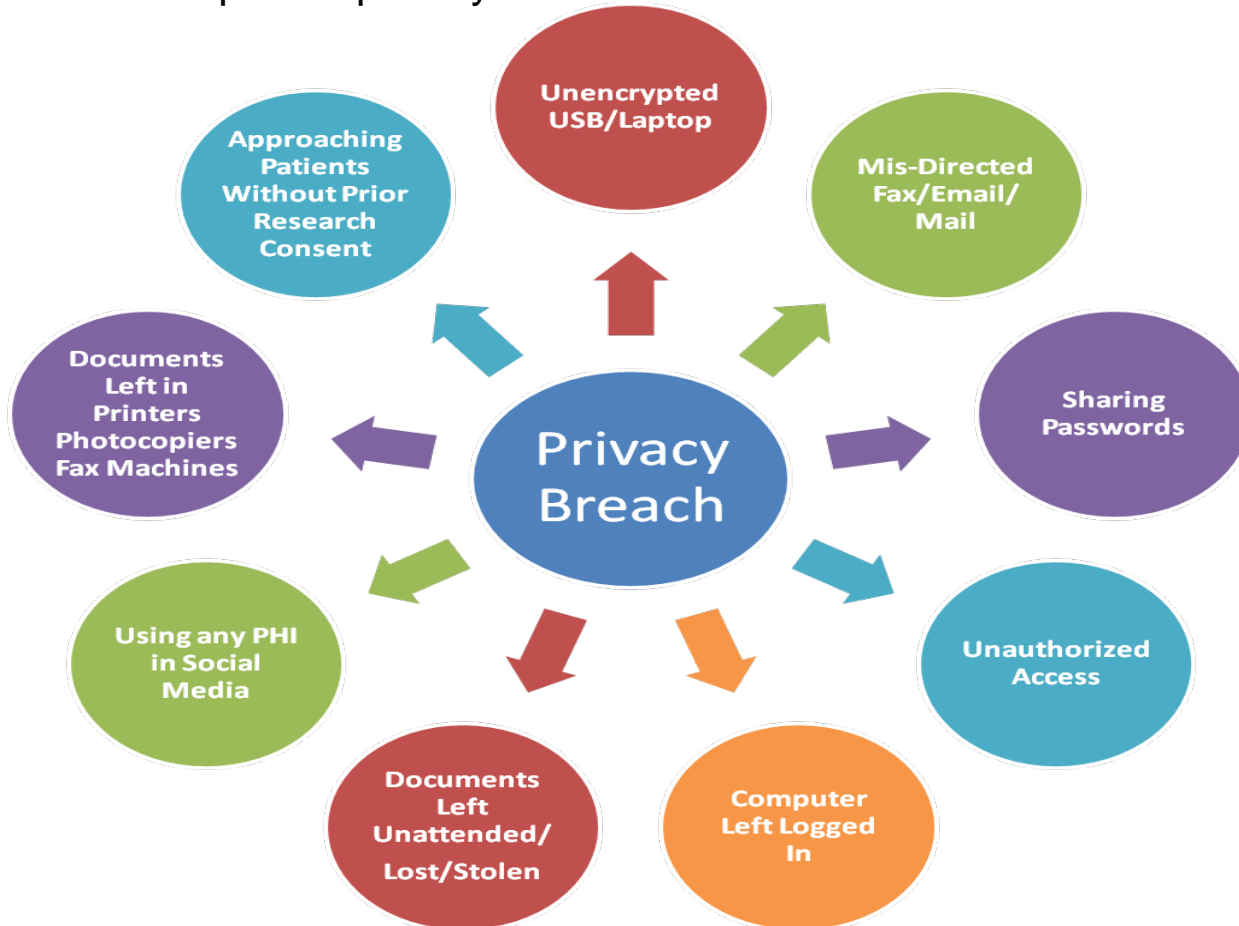
The unauthorized access, collection, use, or disclosure of any personal information or personal health information.

- A breach may be intentional or unintentional.
- Breaches may harm the individual and damage the reputations of the Institute, the Researcher, and/or the staff involved.
- Breaches weaken the trust of the public and our study participants, affecting their willingness to participate in research.
- Corrective action requires time and money, for example, each individual with data breached must be notified.



Respecting Privacy, Safeguarding Data, Enabling Trust

This picture shows examples of privacy breaches.





Reporting a Privacy Breach

- There is a legal obligation to report a suspected or known breach of privacy
- Report to the Director of Quality and/or your Manager and/or the Manager, Clinical Research Compliance and Support
- The TOH policy contains sanctions outlining disciplinary actions for privacy breaches. These sanctions have been posted along with these training slides and must be reviewed.
- The process for managing a reported breach is detailed in a “Privacy Breach Decision Tree” included in the Policy.
- Breaches must be reported by UOHI to the Office of the IPC and/or your professional body, if applicable
- Main goal is to learn and prevent a recurrence!



Preventing a Breach – reminders.....

Do:

- Access only info you require, limit access only to those who need it
- Log off when you are finished with your computer
- Store PHI only on a UOHI secure network drive and password protect the document
- Only use UOHI encrypted mobile devices, and only with REB permission
- Separate PHI from research records ASAP, store in locked cabinets/offices
- Shred papers with PHI when no longer required
- Stay informed by reviewing SOPs/policies, completing your annual privacy training and consider optional continuing education, eg: CITI Canada Privacy course

<https://www.citiprogram.org/index.cfm?region=7>

Do Not:

- Discuss confidential info in public areas
- Share passwords, except for shared documents within a study team
- Leave PHI unattended where it can be viewed by unauthorized users, including an open computer terminal
- Store PHI on personal C drive or mobile devices
- Surf information for your friends or family – this is an automatic “intentional” breach and results in the most severe disciplinary action and significant personal fines!
- Contact patients without their expressed consent
- Release documents (ie: CRFs, logs) containing personal identifiers



UNIVERSITY OF OTTAWA
HEART INSTITUTE
INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

***Please respect the trust your study participant places in you
.....not only for care and safety, but also for protection of privacy!
Before you act, please.....***



Our patients' privacy is in your hands



UNIVERSITY OF OTTAWA
HEART INSTITUTE
INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Contact Information

If you have any questions or concerns please contact the

Clinical Research Compliance and Support office at

clinicalresearch@ottawaheart.ca



UNIVERSITY OF OTTAWA
HEART INSTITUTE

INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

NEW Reporting Requirement

Serious Adverse Drug Reactions and Medical Device Incidents



Acknowledgment: Educational Support for Mandatory Reporting. Health Canada; 2019.



Learning Goals

- 1. Be able to define Serious Adverse Drug Reactions (Serious ADR) and Medical Device Incidents (MDI).**
- 2. Know why Health Canada requires all hospitals to report Serious ADRs and MDIs.**
- 3. Describe the reporting process, including who to notify and where to report.**
- 4. Review case examples.**
- 5. Successfully complete Classmarker Quiz.**





Learning Goal 1:

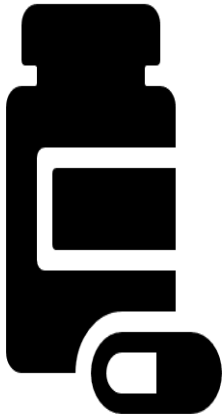
DEFINE



What is a Serious Adverse Drug Reaction (Serious ADR)?

A **serious adverse drug reaction (serious ADR)** is an unintended response to a drug that occurs at any dose and that:

- requires in-patient hospitalization or prolongation of existing hospitalization
- causes congenital malformation
- results in persistent or significant disability or incapacity
- is life-threatening (ie: patient was at risk of death. This does not refer to a reaction which hypothetically might have caused death if it were more severe.)
- results in death
- **requires medical intervention to avoid any of the above outcomes.**





What is a Medical Device Incident (MDI)



A **medical device incident (MDI)** is a death or serious deterioration in the state of health* of a patient, user, or other person caused by:

- A failure of a medical device
- A deterioration in its effectiveness
- Any inadequacy in its labelling or in its directions

Note: Near Misses involving devices are also reportable MDIs.

*life-threatening disease, disorder or abnormal physical state, permanent impairment of a body function or permanent damage to a body structure, or a condition that necessitates an unexpected medical or surgical intervention to prevent such a disease, disorder or abnormal physical state or permanent impairment or damage.



Therapeutic Products to Report

The mandatory reporting requirements for hospitals apply to:

- **Pharmaceuticals**
 - Prescription and non-prescription drugs
- **Biologic drugs**
 - Biotechnology products, fractionated blood products, plasma proteins, and vaccines, etc.
- **Radiopharmaceutical drugs**
- **Disinfectants**
 - chlorhexidine, surgical scrubs, labelled with a DIN
- **Medical devices**
 - ie: hospital beds, infusion pumps, ICDs, external pacemakers, etc.
- **Consumables**
 - IV's, tubing, dressing trays, bandages, bioglues, etc.



Learning Goal 2:

**KNOW WHY TO
REPORT**



Vanessa's Law (*Protecting Canadians from Unsafe Drugs Act*)

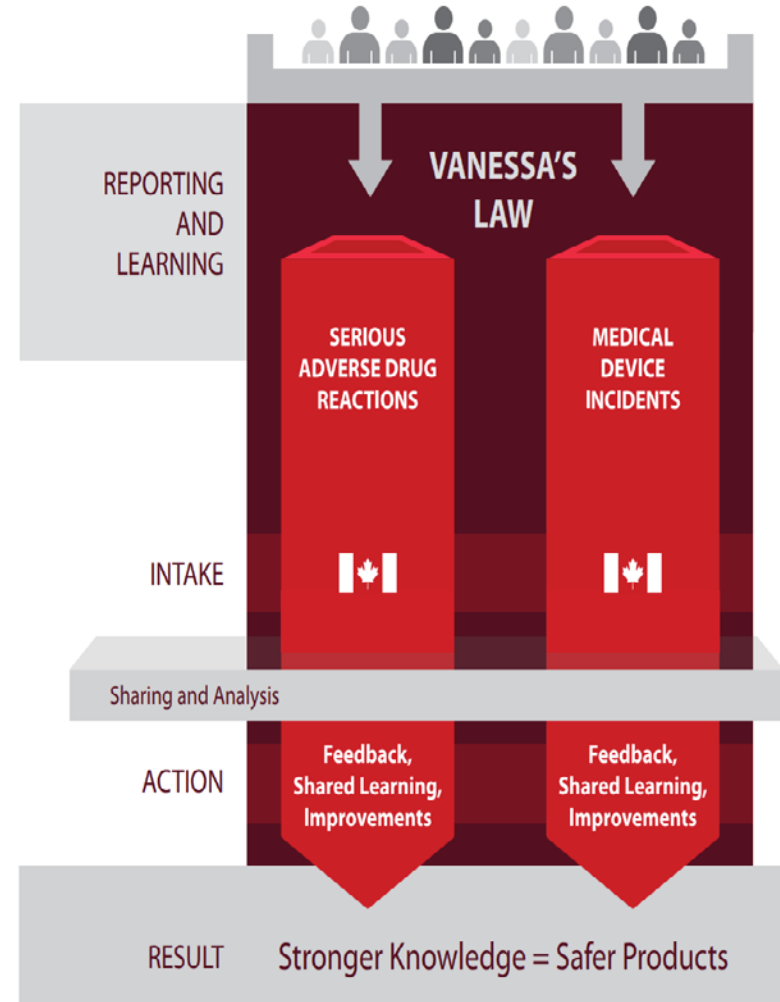


- Vanessa Young died in 2000, at the age of 15, of a cardiac arrhythmia after taking cisapride (Prepulsid®) as prescribed.
- A campaign for increased regulation of therapeutic products, headed by Vanessa's father, subsequently led to greater powers for Health Canada to request safety data from hospitals and industry about drugs and medical devices.
- **Vanessa's Law** was enacted in 2014 and the mandatory reporting requirements come into effect on December 16th, 2019.



Why is Reporting Important?

- Health Canada is always looking for ways to strengthen its knowledge base on product safety in the interest of improving patient outcomes and public health.
- Serious ADR and MDI reports are important sources of information for identifying emerging safety issues.
- Serious ADR and MDI reports help us learn from incidents and make improvements to safety such as labelling changes, product information updates, or recalls.





Legal Obligation to Report



- **All** hospitals must report Serious ADRs and MDIs to Health Canada.
- Reports must be made **within 30 calendar days** of first documentation of the Serious ADR or MDI within the hospital.
- All hospitals must report to Health Canada even if the incident happened at home or at another hospital.



Learning Goal 3:

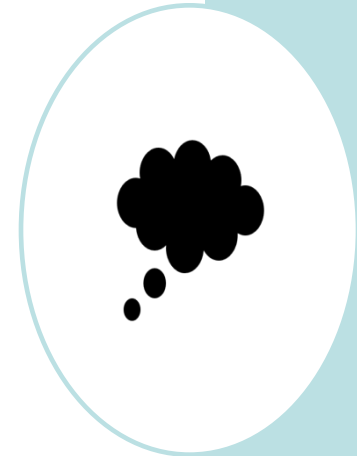
REPORTING



When in doubt, Report!

- **Report any suspicions, even if:**

- You aren't 100% sure of the root cause.
- You don't have all of the details yet.
- The incident was a Near Miss, but could have caused death or serious harm (for MDIs only).



Quick Tips: Identifying a Serious ADR or MDI



- Serious harm from a drug or from a medical device can be mistaken for a symptom of a disease.
- A high level of suspicion, clinical awareness, and patient dialogue are key components in identifying a serious ADR or MDI.
- A serious ADR or MDI can occur shortly after beginning treatment or much later.

Quick Tips: Making an Assessment

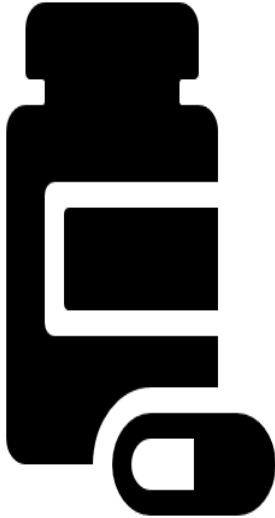


An incident may be a Serious ADR or MDI if there is:

- An unexpected change in the patient's health condition
- A new health problem
- A need for new urgent therapies, procedures or surgeries
- Sudden need for a rescue drug, such as naloxone, epinephrine or glucagon
- A medical order for an acute change to therapy



Reporting Process – Serious ADR



✓ Notify

- Your Clinical Manager or the Nursing Coordinator

✓ Report in SLS



Reporting Process – MDI

✓Notify

- Your Clinical Manager or the Nursing Coordinator
- Biomed (Business hrs x17447; Off-hrs call the Bunker and ask them to page Biomed on-call)

✓Report in SLS

✓Take the equipment out of service:

1. Place smaller item(s) in unit's drop-box for pick up and attach a "request for service" tag, found with the drop-box.
 - Ref# is the SLS Report #
2. Call a porter to take the equipment to Biomed.



BIOMEDICAL ENGINEERING **MEDICAL DEVICE INCIDENT**

Ref. # _____

HOSP 207 (10/2019)



RESEARCHERS

✓ Notify

- Research Ethics Board if the Serious ADR is also unexpected (as per REB SOPs)
- For MDIs: Biomed (Business hrs x17447; Off hrs call the Bunker and ask them to page Biomed on-call)

✓ Report in SLS

- Reporting SADR and MDI remains unchanged for those that occur in clinical trial participants under a Health Canada approval (CTA with NOL/NOA, ITA), and are the responsibility of the study team to report.
- Reporting SADR for Phase IV drug trials remains the responsibility of the study team, but will be through this new process of disclosing to the Institution for their reporting to Health Canada.

✓ For MDIs: Take the equipment out of service

1. Place item(s) in unit's drop-box for pick up and attach a "request for service" tag, found with the drop-box.
2. Call a porter to take the equipment to Biomed.



Report Form

1. The person who discovers the serious ADR or MDI is responsible for reporting it in the Safety Learning System (SLS).
2. SLS will be updated to include new data fields for Serious ADR and MDI. **Please be sure to complete these fields.**
3. Once in SLS, the report is sent to Quality & Patient Safety to complete the final submission to Health Canada on behalf of UOHI.




Learning Goal 4:

CASE EXAMPLES



Case Example 1

A patient had been taking warfarin, among other medications, and presented to the emergency department with a life-threatening gastrointestinal bleed. The patient required hospitalization in order to be stabilized.

 Report

Life-threatening
condition

Hospitalization



Case Example 2

A patient experienced dizziness and sweating after a dose of insulin. The patient required glucose tablets to recover. It was discovered that a short-acting insulin had been provided instead of the patient's usual long-acting insulin.



NOT a Serious ADR

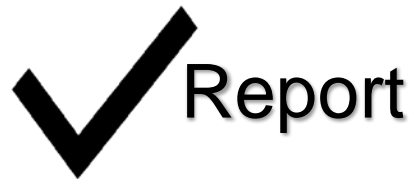


This is a medication error (patient given wrong drug) and should be reported in SLS as such, rather than as a Serious ADR. Med errors such as this are preventable.



Case Example 3

A health care professional reported that the sewing cuff was discovered to be defective during a heart valve implant. The defective valve was abandoned, a new valve was implanted, and pumping time during surgery was extended. This defect had the potential to cause serious harm.



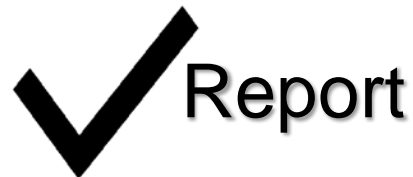
Potential for death or serious deterioration due to extended surgical time.

Possibility that defect could have been missed prior to close on other patients, leading to emergency failure.



Case Example 4

A patient is admitted to hospital in hypoglycemic shock. The patient thinks that he was using his glucose strips properly. The nurse realizes that the patient had been using a batch of out-of-specification blood glucose test strips released by the manufacturer. The readings provide incorrect values leading to incorrect insulin dosages.



Serious deterioration
in the state of health
of a patient.

Report even though
patient was not
hospitalized when
the strips were
used.

Even though it's possible that the patient was either non-compliant or not using the test strips correctly, since the testing strips are out of specification, it is reasonable to suspect that this caused the hypoglycemic shock and to report it. Staff are not required to get to the root cause before reporting.



Case Example 5

A user performed an inflation test prior to inserting the balloon catheter into the patient, as required in the instructions for use accompanying the device. A malfunction on inflation was detected and another balloon was used.



Inflation test is part of the standard procedure prior to patient use to look for deficiencies and avoid patient harm.



Clinical Research Privacy & Serious Adverse Drug Reactions and Medical Device Incidents Quiz

- Please Note: The *Clinical Research Privacy Quiz* and the *Serious Adverse Drug Reactions and Medical Device Incidents Quiz* have been combined into one.
- Please click [here](#) to take the quiz.
- Save a copy of your completion certificate for your records and send to Human Resources.