Barrie and Community Family Health Team

All User Privacy Training

Privacy training focused on ensuring and maintaining the trust and privacy of our patients

Ontario

Barrie and Community Family Health Team

Outline

- Conflict of Interests , Presenters & Objectives
- Privacy Basics & Principles
- Privacy in Primary Care
- Consent & Access to Information
- The Privacy Officer & the Information and Privacy Commissioner
- Organizational Compliance & Your Role
- Privacy Breaches – Real World Examples
- Security & Safeguards
- Creating a Privacy Culture

Barrie and Community Family Health Team

Conflict of Interests Disclosures

- Faculty: Sean McConnachie, Dr. Anne DuVall & Larry Villemaire
  - Relationships with commercial interests: none

- This program has received financial support the Barrie and Community Family Health Team in the form of refreshments and materials and equipment.
  - Potential for conflict(s) of interest: none

- The information presented in this CME program is based on recent information based on PHIPA. The training materials have been developed based on information supplied by DDO Health Law. DDO Health Law is a firm that provides advice, tools and training to the health care sector. The training will meet the recommended training actions as prescribed by the Information and Privacy Commissioner of Ontario.

Barrie and Community Family Health Team

Prepared by

Sean McConnachie

Manager of QIDS and Assoc. Privacy Officer

- 10yrs of Healthcare experience
- Specialist in healthcare research and public policy

Dr. Anne DuVall

Information and Technology Clinical Lead

- Former Medical Director of the BCFHT
- Family Physician for 30 plus years

Larry Villemaire

Manager of Information and Technology

- Technology and security expert
- Project and quality leader
- 8 years of IT experience
- CompTIA Network+ & Security+ certified

Special Thanks to **Mary Jane Dykeman** (DDO Law) & **Kate Dewhirst** (Kate Dewhirst Law) for allowing us to use materials developed by them for these training sessions

Barrie and Community Family Health Team

Learning Objectives

- At the conclusion of this activity participants will be able to:
  - Identify their own roles and responsibilities to maintain a safe Privacy work environment based on PHIPA.
  - Articulate the BCFHT's breach management process.
  - Apply patient consent and access to information policies.
  - Recognize when and how to report a privacy breach.
  - Reduce the incidence of privacy related issues.

Barrie and Community
Family Health Team

PRIVACY BASICS AND PRINCIPLES

Privacy Theory

Privacy

- The fundamental right of an individual to control information about themselves (including the collection, use and disclosure of and access to that information)

Confidentiality

- The obligation of the health information custodian to protect personal information, to maintain its secrecy and not misuse or wrongfully disclose it

Barrie and Community Family Health Team

What is PHIPA?

- The Personal Health Information and Privacy Act (PHIPA) was established in 2004 to establish rules around the the collection, use and disclosure of personal health information. PHIPA is the legislation that all healthcare providers work under and are obligated by law to follow.

- PHIPA provides specific details around:
  - Patient consent and rights to information
  - What is PHI
  - Who is a HIC and what their responsibilities are
  - What is an Electronic Medical Record and how they should be managed
  - How PHI can be used by various actors

Barrie and Community Family Health Team

What is Personal Health Information?

- Any information collected on an individual or group (oral or recorded) during or for the purposes of providing healthcare.
- Most PHI will be found and stored in health records or medical charts (paper or electronic).
- Anything that has a patient identifier is considered to be PHI. This includes email, written notes, schedules, etc.
- All health information custodians must know where all PHI is stored at all times (e.g., for access requests and notice of information management practices).

Barrie and Community Family Health Team

Who are the Privacy Actors?

- Patients
- Care Givers & Substitute Decision Makers
- Health Information Custodians (HICs)
- Health Information Network Providers (HINPS)
- Prescribed providers & entities
- Agents
- Privacy Officers
- Electronic Service Providers
- Information & Privacy Commissioner of Ontario
- Ministry of Health and Long-term Care
- Private insurers
- Researchers

Barrie and Community Family Health Team

What and Who are HICs?

- Health Information Custodians (HICs) are responsible for the collection, use and disclosure of personal health information (PHI) that is collected on behalf of their patients.
- HICs are generally institutions, facilities or private practices that are designated by the provincial government to provide health care.
  - Hospitals
  - Individual or group healthcare providers
  - Laboratories
  - Ambulance services
  - Pharmacies

Barrie and Community Family Health Team

What and Who are HIC Agents?

- An agent under PHIPA, is an one that has been contractually authorized by a HIC to work on the behalf of the HIC with PHI. Agents are obligated to ensure that the requirements of PHIPA are achieved on behalf of their HIC.

- Agents include:
  - Employees of a HIC
  - Person contracted to work on behalf of a HIC
  - Students and volunteers
  - Specialists and third-party groups

What and Who are HINPs?

- PHIPA allows for HICs to use electronic health records (EMR) to for the collection, retention and use of PHI. HICs are also allowed to work together to provide greater access to PHI to improve care for patients.
- Health Information Network Providers (HINPs) are organizations that provide EMR services to HICs.

Barrie and Community
Family Health Team

PRIVACY IN PRIMARY CARE

Barrie and Community Family Health Team

So who is responsible for what?

- In primary care, individual physicians are considered to be HICs and are responsible for privacy and confidentiality of their PHI.
- The BCFMC is considered its own HIC and the physicians who work there are considered agents of the BCFMC.
- The BCFHT and FHO are considered to be both a HICs and a HINP, resulting in overlapping roles and responsibilities.

Barrie and Community Family Health Team

The Joint Venture Agreement

- The BCFHT and each member physicians of the FHO are signatories to the Joint venture agreement. This agreement was created to establish the EMR, and to outline roles and responsibilities.
- Physicians and the BCFHT are both responsible for privacy in physician practices and the EMR.
- The BCFHT is designated with the responsibilities of the Privacy Officer.
- Among other things, the agreement outlines who has access to what information where.

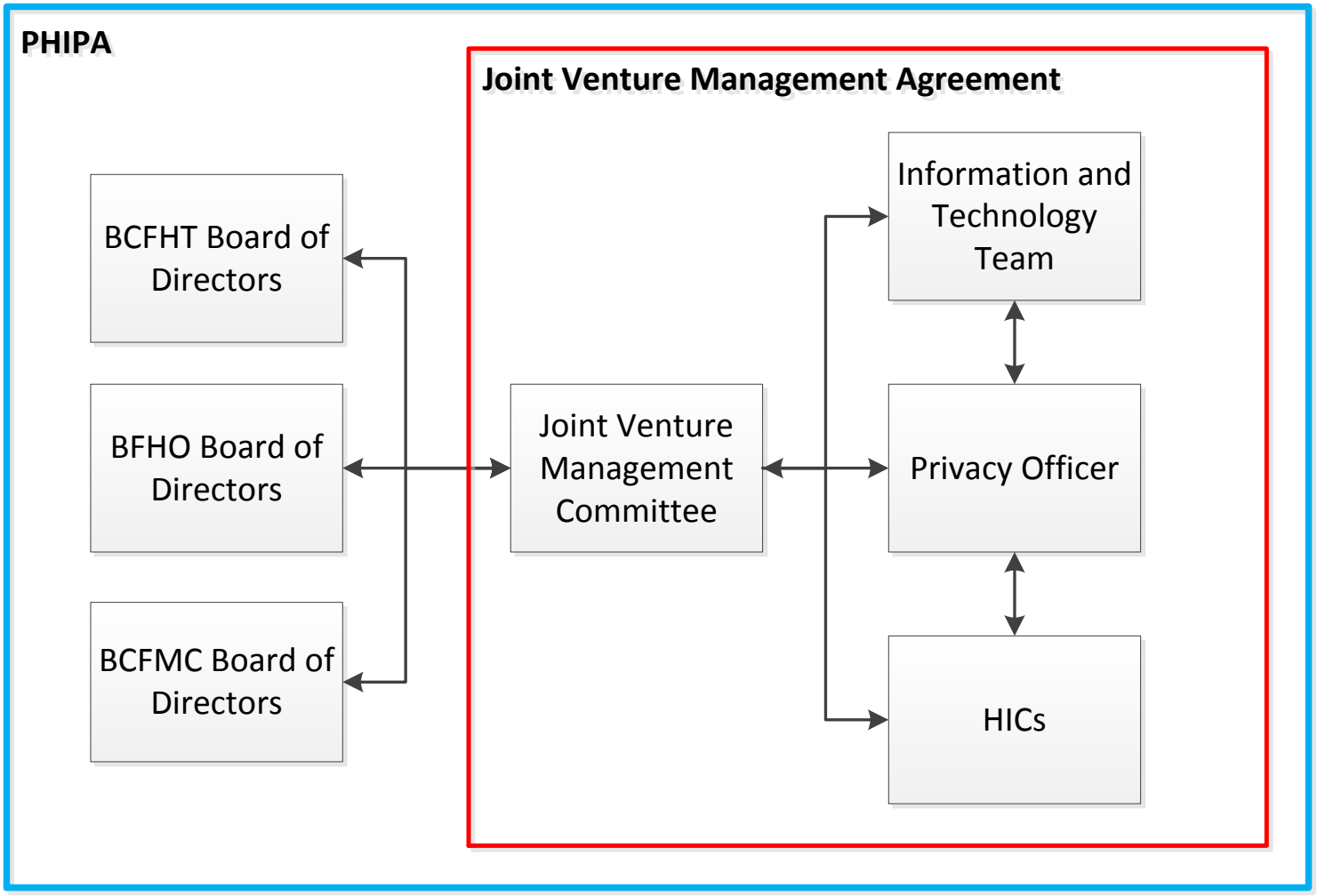
Barrie and Community Family Health Team

Who Makes up our Privacy Team?

- **Joint Venture Privacy Officer,** Michael Feraday
- **Associate Privacy Officer,** Sean McConnachie
- **Manager of Information and Technology**, Larry Villemaire
- **Clinical IT Lead,** Dr. Anne DuVall
- **The Joint Venture Management Committee**
- **Boards of Directors**

Barrie and Community Family Health Team

How are We Structured?



Barrie and Community
Family Health Team

CONSENT AND ACCESS TO INFORMATION

Patient Rights

All patient, subject to some exceptions, have rights to:

- Consent (or withhold or withdraw consent) to the collection, use or disclosure of PHI
- Have access to PHI (regardless of where it is kept)
- Ask for a correction to a record of PHI
- “Lock” or “Masking” PHI from health care providers for health care purposes.
- See who has accessed their PHI and why.

Barrie and Community Family Health Team

Patient Consent

Can't collect, use or disclose PHI unless:

- Individual consents and the collection, use or disclosure is necessary for a lawful purpose, or
- The collection, use or disclosure is permitted or required by PHIPA or another Act

Can't collect, use or disclose:

- If other information will serve the same purpose
- More information than is necessary for purpose

Barrie and Community Family Health Team

Patient Consent

Implied Consent

- Is considered the granting of permission by patients without a formal agreement between them and a healthcare provider.
- When a patient makes an appointment with a healthcare provider consent is implied to receive care.
- This is also true with the use of healthcare information if there is public notification of the use of this information.

Patient Consent

HIC may use PHI without consent for:

- Billing
- Risk management & quality initiatives
- Planning programs
- Teaching your agents
- Privacy audits
- IT activities

- Discretion to warn – may disclose PHI to eliminate or reduce a significant risk of serious bodily harm

Barrie and Community Family Health Team

Removal of Consent

- Individuals have a right to make choices about their personal health information
- One way that individuals can exercise this choice is to ask to use a “lockbox” or “masking” to:
  - Hide clinical information from health care providers at HIC (**Restricted Use**) or
  - Not disclose clinical information to external health care providers for health care purposes (**Restricted Disclosure**)
- However, patients can not completely limit access to their PHI.

Barrie and Community Family Health Team

How Old do you need to be to Consent?

AGE	CAPACITY	DECISION-MAKER
Person of any age	If capable	Can make decisions about release of everything in his/her own health record; can also delegate this decision (in contrast to treatment decisions, which cannot be delegated)
Person of any age	If incapable	Needs a substitute decision-maker to release anything in health record
Up to age 16	If capable	Can make decisions about release of everything in his/her own health record AND A parent can also consent to release of information about any treatment or counseling that child did not consent to on his/her own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS

Barrie and Community Family Health Team

The Circle of Care

- Patient information can be disclosed to others healthcare professionals or organizations, without the expressed consent of a patient, for the purpose of providing healthcare for that patient.
- This only includes those who are actively involved in the care of a patient.

Look and don't tell, listen and don't tell

Barrie and Community Family Health Team

Access to Information

Patients own their health information, the Health Information Custodians do not.

- We are all required to provide access or copies to PHI for patients.
- We are required to provide this access within 30 days of a request being made.
- Patients have the right to change information in their medical record that they believe is in accurate.
- Patients allowed access to all information that has personal identifiers in it (i.e. charts, notes, emails, etc.)

Barrie and Community Family Health Team

Fees for Access

We are allowed to charge patients fees for access to their information.

- Fees must be representative of the time and material costs associated with the access.
- Fees must be considered reasonable and inline with fee regulations.
- Fees can not be prohibitive for patients to access their own PHI.
- The BCFHT does not charge patients to access their PHI.

Barrie and Community
Family Health Team

THE PRIVACY OFFICER AND THE INFORMATION AND PRIVACY COMMISSIONER

Barrie and Community Family Health Team

Role of the Privacy Officer

- The Privacy Officer's role is established by the Joint Venture agreement and their authority is outlined within the agreement
- The Privacy Officer's roles and responsibilities include, but are not limited to:
  - Ensuring all parties compliance with PHIPA
  - Staying aware of changes in legislation and decisions from the IPC
  - Ensuring that all parties are properly informed of their duties under PHIPA
  - Responding to privacy inquiries from the public
  - Investigating any privacy breaches
  - Working with the IPC on any major investigations

What is Role of the Information and Privacy Commissioner

- Oversees compliance with PHIPA, including launching investigations
- Educates and informs HICs, patients/clients/residents and the general public
- Deals with complaints
- May offer limited comments on HICs' information practices
- Works with peers in other jurisdictions

Barrie and Community
Family Health Team

ORGANIZATIONAL COMPLIANCE AND YOUR ROLE

Barrie and Community Family Health Team

Responsibilities of Our Teams

The main responsibilities of all of our teams are to:

- Be aware of and follow all the rules established by PHIPA and the IPC
- Ensure the privacy and confidentiality of our patients
- Ensure that we are all following the rules of the Joint Venture Agreement
- Ensure that they are following all IT policies and EMR user agreement
- That we are mindful of the privacy outcomes of our actions or inactions
- Report and deal with all privacy breaches that occur
- Work with patients and the public to fulfill all privacy requests that we receive

Privacy Auditing

- In 2016-17, the provincial government introduced amendments to PHIPA that specifically speak to the need to conduct ongoing audits of electronic medical records.
- Based on this and recommendations from the IPC, JVMC has directed the BCFHT to conduct random audits of user accesses to PHI starting in October 2017.

Barrie and Community Family Health Team

Privacy Auditing

- These audits will be conducted twice a year (October and April) with the possibility of higher frequencies in the future.
- The audits will be conducted by the Privacy Team with the aggregate results of these audits being presented to the JVMC and the Boards.
- The Privacy Team will investigate any major breaches that it may find.

Privacy Auditing

- These privacy audits will focus on, but may not be limited to:
  - All activities of randomly selected users for a given period;
  - The monitoring of specific patient profiles on an on-going basis
  - The monitoring of personal and family records on an on-going basis

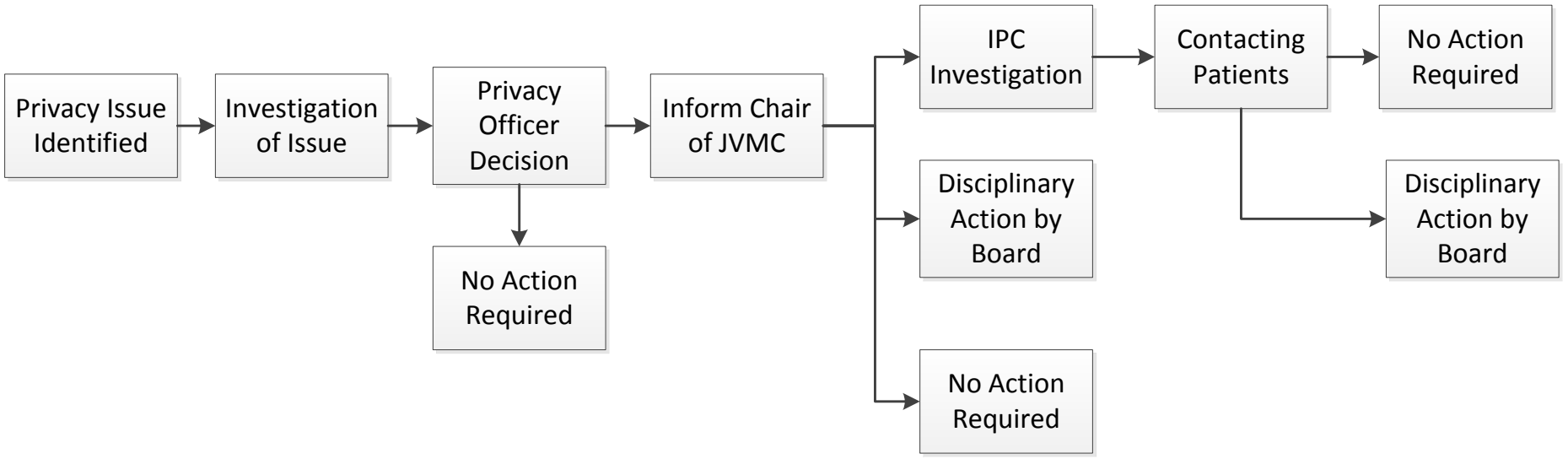
Barrie and Community Family Health Team

Types of Breaches

		Outcome	
		Minor	**Major**
Motivations	**Accidental**	This are breaches that can occur on a daily basis and are slip ups. No major action will be taken. Ex. Talking to a patient about they medical condition in front of others.	These are breaches that require action by the organization, but will not result in disciplinary action, as they are accidental. Ex. Improper disposal of health information.
	Intentional	These are breaches that do not necessarily compromise patients, but are completely preventable as they are intentional. Follow-up with the perpetrator will occur, and if this is a reoccurring issue, disciplinary action will be taken. Ex. Sharing or using some else's password	These are breaches of the highest order and will require a response from the organization and will result in disciplinary action, including removal from the BCFHT. Ex. Snooping or sharing PHI with someone not in the circle of care

Barrie and Community Family Health Team

How Privacy Issues are Dealt with



Barrie and Community Family Health Team

Consequences of a Breach

- Public investigation of a breach by both the BCFHT and the IPC.
- Fines of between $25K to $500K levied by the province based on the recommendation of the IPC.
- Termination of employment.
- Open to litigation by those that are affected

Barrie and Community Family Health Team

Reporting to your College

- Depending on the severity of the privacy issue and the person's complicities in it, the BCFHT is mandated to inform your college.
- The college will conduct its own investigation based on information provided the BCFHT.
- The college can and will permanently remove members depending on the severity or reoccurrence of the issue.

Barrie and Community Family Health Team

What can you do?

- Be mindful of privacy and confidentiality in your day-to-day activities.
- Understand the rules and regulations around patient privacy.
- If you are involved with or notice a breach, report it immediately.
- If you have any privacy questions, reach out to the Privacy Officer.

If in Doubt, err on the side of More Privacy not Less

PRIVACY BREACHES – REAL WORLD EXAMPLES

Getting Drugs

- A 58 year old nurse has been arrested for accessing patient information in order to acquire narcotics.
- The nurse was using patient information to make false prescriptions for the hospital's in-house pharmacy.
- The nurse is currently in court proceedings, and has been removed from the hospital and her college.

Barrie and Community Family Health Team

Out with the Old

- FHT employee accidentally threw out medical records. Privacy Team was notified as soon as possible and was able to contain the issue.
- The Privacy Team dumpster dove in order to recover the records and actually found multitudes of other PHI.
- No action was taken against the staff member.

Barrie and Community Family Health Team

Student Snooping

- A Master's of Social Work Student who was working with a FHT on a placement was found to have accessed 139 patient records for patients who were not within their circle of care.
- The student was fined $25,000 by the province and is now open to potential civil suits.
- This person will not be able to enter into the College of Social Workers.

Barrie and Community Family Health Team

I’m a Doc, so Why not

- Physician and their staff were accessing their own medical records on a routine basis.
- Physician was ordering lab tests and prescriptions for themselves.
- All colleges and the EMR Users terms of agreement absolutely prohibit accessing your own records, prescribing any drugs or ordering any tests.

Just Checking In

- $3.5M Class action law suit against hospital and specialist for the snooping of a single employee.
- Assistant of the specialist used her access to review medical records of family members and friends.
- Plaintiffs allege that privacy policies and procedures were “inadequate, underfunded and under enforced”.

Barrie and Community Family Health Team

So Long Binder

- FHT employee accidentally left a binder behind at a group session outside the building. The staff member didn't notify the Privacy Team until 48 hours had passed.
- The Privacy Team was not able to recover the information and a formal investigation occurred. All patients were informed of incident.
- No disciplinary action occurred to the staff member.

Barrie and Community Family Health Team

Who's the Boss?

- Parents of a child going through a divorce wanting to influence the other parent's access to a child's health information.
- Any parent trying to change the other's access to health information requires a separation agreement or court order.
- No separation agreement or court order available, both parents have access to the child's health information.

Barrie and Community Family Health Team

Locked Out

- Patient came into clinic but health record was locked. Clinic team was unable to access the record and provide its best care.
- Patient was very upset and stated that they did not request a locking of their chart.
- Physician that locked chart had a written and signed request from patient to lock chart. Patient decided to continue lock on chart.

Barrie and Community Family Health Team

On a Disc, but no Disc

- Physician used USB keys to save files from the EMR to take them home to review on home PC. Lost the USB key somewhere during their commute home.
- The key was not recovered, patients were informed of information lost. EMR was able to tell us what patient information was accessed and saved.
- IPC was notified and no further action was required.

SECURITY AND SAFEGUARDS

Barrie and Community Family Health Team

HIC RESPONSIBILITIES

- Must take steps that are “reasonable in the circumstances” to ensure that Personal Health Information in HIC’s custody is protected against theft, loss, and unauthorized use or disclosure and ensure that records containing PHI are protected against unauthorized copying, modification, or disposal.
- Must ensure that PHI records are retained, transferred, and disposed of in a secure manner and in accordance with prescribed requirements.

Barrie and Community Family Health Team

SAFEGUARD EXAMPLES

LOCK ACCURO WHEN AWAY FROM THE PC

- If you are stepping away from an Accuro session, always lock it down (ALT-F12 by default).

NEVER SHARE YOUR PASSWORD OR ACCOUNT INFORMATION

- It is absolutely forbidden to share your account information with someone else, or to use someone else's account to login to the EMR. Inform IT immediately if an account is to be terminated.

DO NOT EMAIL UNENCRYPTED PATIENT INFORMATION

- Email is not a secure method of communication NOTE: This includes emailing IT support – there is a unique File Number in Accuro for each patient record; use that instead of patient name and health card number.

SAFEGUARD EXAMPLES

PATIENT DATA MUST NOT BE HELD OUTSIDE OF A SECURE LOCATION

- You should never copy patient information outside of the EMR (such as to a local hard drive, USB drive, or other media). If information must be copied outside of the EMR, it should always be encrypted.

ALWAYS DISPOSE OF PATIENT INFORMATION PROPERLY

- If you have patient information on paper, or a disc, or some other media that needs to be disposed of, do so securely. Acceptable disposal means information must be cross-shredded, pulped, pulverized, or incinerated.

NEVER STORE PERSONAL HEALTH INFORMATION IN THE CLOUD

- Services like Dropbox, Google Docs, One Drive, etc. are generally based in the USA. Their laws regarding privacy are different from those in Canada and may not protect information stored there.

Barrie and Community Family Health Team

PHYSICAL & VIRTUAL SECURITY

ANTIVIRUS SOFTWARE

- The FHT and the FHO use an application called ESET to provide protection against malware. Unfortunately, no software can provide 100% protection against all threats. Use common sense – be cautious with unexpected email attachments or visiting suspicious websites; they are often vectors for malware.

FIREWALLS

- We use both hardware and software firewalls to provide controls on data coming into and going out of our network.

VIRTUAL PRIVATE NETWORKS

- These provide a secure method of transmitting sensitive data across public networks (like the internet). All FHT and FHO sites are interconnected using these VPNs to allow secure transmission of files (e.g. FHT file share servers and Accuro CloudSync) and for IT to track hardware, software, and provide support.

Barrie and Community Family Health Team

PHYSICAL & VIRTUAL SECURITY

RESTRICTED FACILITY ACCESS

- Office spaces where paper documents, computer systems, fax machines, etc. are stored (especially containing PHI) should be locked down from unauthorized access. Alarm systems, passcards/fobs, etc. are also recommended.

SECURE DOCUMENT CASES

- If you must transport paper documents containing PHI, it should be in a lockable bag or case.

BACKUPS

- All EMR and FHT/IT/CLINICS servers are backed up in data centres. Anything stored locally (e.g. the C drive) is not backed up, so never store anything critical there. PHI should NEVER be stored on local or removable media.

Barrie and Community
Family Health Team

CREATING A PRIVACY CULTURE

New User Orientation

- In collaboration with the IT Team and their Accuro training, the Privacy Team will be running quarterly privacy sessions for all new EMR Users.
- The Privacy Team has also created up-to-date privacy pledges that are part of the *New User EMR Package*.

Barrie and Community Family Health Team

Privacy Pledges

- The BCFHT has all of its staff members sign an annual privacy pledge the reaffirms each persons commitment to not only maintaining the privacy and confidentiality of the organization and other staff, but of all our patients and their families.
- It is recommended by the IPC that all HICs conduct annual privacy pledges to keep privacy front of mind of all peoples that handle PHI.

Barrie and Community Family Health Team

It Starts with You!

- Privacy and confidentiality are not the responsibilities of a single person, we are all individually responsible for our own actions.
- Privacy needs to be at front of mind in everything that we do as we all will be held to account for our own actions.

Barrie and Community Family Health Team

We are here to help

- We are not looking to get anyone in trouble. Our main concerns are ensuring that we all have the legitimacy to continuing the good work we do.
- The sooner we know about an issue, the sooner we can contain it and mitigate the impact of it on everyone involved.
- If you every have any privacy questions, contact us

  Email: accessprivacy@bcfht.ca

  Phone: 705-721-0370 x2135