

**Manager and Medical Director’s Privacy and *PHIA* Toolkit**

**Why the focus on Privacy now?**

On **June 1, 2013**, the ***Personal Health Information Act* *(PHIA)*** and its regulations will be **law in Nova Scotia**. Like health privacy legislation in other Canadian provinces, this new law will govern the collection, use, disclosure, retention, disposal and destruction of personal health information at Capital Health. The Act recognizes the rights of individuals to protect their personal health information and control its collection, use and disclosure. *PHIA* requires consent in many situations and grants individuals the right to access their personal health information, subject to limited legal exceptions. The Act permits Capital Health to manage personal health information to provide, support and manage health care in accordance with *PHIA* requirements.

**NOTE: Capital Health takes its responsibility to protect personal health information seriously and we are all legally and publically accountable for the actions we take to safeguard information.** Capital Health’s CEO and other Senior Leadership recently appeared before a Public Accounts committee of MLAs to discuss our practices, after the auditor general’s report 2012. To view the video or read the transcript, goto:http://nslegislature.ca/index.php/committees/committee\_hansard/C7/

**What is included in this toolkit?**

1. FAQs for Managers and Medical Directors
2. FAQs for Staff
3. Updated Confidentiality Pledge
4. Group education/discussion materials
5. DRAFT User Access Auditing and Record of User Activity policy
6. Written Privacy Statement
7. Notice of Purposes Document
8. PHIA readiness Checklist for Managers and Medical Directors
9. 1 page Privacy Quick Reference Guide
10. Commonly referenced CDHA policies relating to the privacy, confidentiality and security of

personal health information

1. **FAQs for Managers and Medical Directors**

**What is the “Capital Health Protects Patient Privacy…It’s the Law” Campaign?**

While *PHIA* reflects many existing privacy norms at Capital Health, there are a number of **new** requirements and changes that affect how we manage personal health information at Capital Health. **All staff, physicians, learners, volunteers, etc. must be aware of them.** These changes will impact direct **clinical care, teaching, research and quality improvement activities** at Capital Health, amongst others.

The Nova Scotia government announced the implementation date and regulations for *PHIA* in December 2012. Given the diversity of Capital Health and its services, a *PHIA* Implementation Committee with representation across the organization has been meeting to assist in identifying organization level compliance gaps and policy changes.

Having presented to leadership and various units in the last few months, we are intensifying our efforts to build awareness of *PHIA* across Capital Health before June 1st. May will see a month long awareness campaign that will include the availability of a LMS education course, staff awareness posters, a series of district wide presentations open to all staff, and updated policies and procedures, including a new user access auditing policy, in addition to this toolkit.

**How will Capital Health educate staff, physicians, etc about their privacy responsibilities?**

* **Mandatory LMS Course:** Given Capital Health has over 11,000 staff, physicians, learners and volunteers, a mandatory LMS Course will be the primary vehicle for education. It is available now on the CDHA LMS as well as the provincial elearning website and should be completed as soon as possible. We will monitor compliance and provide managers with an update by July 31st, 2013 of who has completed the course. New staff, learners, etc will complete it at orientation and it will be done annually.
* Individuals can access the LMS course and the Course/Confidentiality Pledge reaffirmation survey question by going CDHA’s LMS system at <http://lms.cdha.nshealth.ca> If you log in to LMS and select Privacy and Confidentiality from the Catalogue menu, you will find the Personal Health Information Act Privacy and Confidentiality Course and the Pledge of Confidentiality Reaffirmation that you are required to answer after taking the course.  You must take BOTH parts.

**\*\*NOTE \*\*Full step by step instructions are included at the end of the staff FAQs (pg 16 of this toolkit).**

* + **Managers who want to teach the course as a classroom session for staff:** You can present the course in a team session. Please ensure that you have recorded the names and employee numbers for staff attending. Please forward the list of names to the Privacy Officer by email at privacy@cdha.nshealth.ca or by fax to 473-7850.
	+ Attend PHIA information sessions. A list of current scheduled sessions is included in this toolkit and look for advertisements as to additional sessions in the future.

Individuals who do not complete the LMS course in a timely manner may have his or her access to systems containing personal health information suspended.

**NOTE:** We are required by *PHIA* to educate everyone authorized by Capital Health to act on its behalf of their responsibilities regarding personal health information. Even those who may not handle personal health information regularly may find a missing piece of personal health information or may be approached by a patient for help and learn details of their situation. They must know how to safeguard personal health information.

* **New Confidentiality Pledge:** Everyone as part of completing the course will have to affirm their confidentiality pledge, which has been updated. A copy is attached to this toolkit for you.
* **Updated Policies:** In addition, updated privacy and release of information policies will be in place by the end of May for reference, as well as policies and procedures around the conduct of research. There will also be a new user accessing auditing policy. This policy will require managers and medical directors to investigate audit reports of their staff’s access to electronic information systems containing patient information to verify the access in question was legitimate. A final draft of the auditing policy, which is before Senior Leadership, is attached.
* **Information sessions:** Information sessions /lunch and learns with Capital Health’s Privacy Officer will be held at a variety of sites in May and are open to everyone. Where the technical ability exists, the LMS will be conducted for attendees as a classroom session by the Privacy Officer. A schedule of presentation times are below:
1. Hants Community Hospital – May 7th -12:00pm to 1:00pm; 2:00pm to 3:00pm; both sessions in Room 114A
2. Cobequid Community Health Centre –May 8th - 11:30am to 1:00pm; Room 3127
3. Twin Oaks Memorial Hospital -May 9th - 12:30pm to 1:30pm; Boardroom
4. Musquodoboit Valley Memorial Hospital - May 9th12:30pm to 1:30pm; Boardroom via Telehealth
5. Eastern Shore Memorial Hospital – May 9th - 12:30pm to 1:30pm; Telehealth Room, 2nd Floor; and

May 13th – 12:30pm to 1:30pm; 2:00pm to 3:00pm, multipurpose room, 1st floor

1. Dartmouth General Hospital-May 14th, 11:00am to12:00pm; 12:00pm to1:00pm; both sessions are in Boardroom 1608
2. Nova Scotia Hospital –May 15th- 12:00pm to1:30pm - Hugh Bell Lecture Hall
3. Halifax Infirmary – May 16th – 12:00pm to 1:30pm - Royal Bank Theatre
4. Victoria General – May 17th- 12:00pm to 1:30pm-VG Auditorium
5. Public Health – May 22nd- 2:30pm to4:00pm - Community Room, Burnside
6. Continuing Care – May 29th – 10:00am to 12:00pm, Room 217, Joe Howe
7. East Coast Forensic Hospital – June 19th – 12:30pm to 1:30pm, Blue Room
* **Poster Campaign:** A Poster campaign reminding staff of the legislation and the importance of protecting patient privacy will also happen in May. Copies of the posters are attached.
* **Intranet Site:** Materials will be made available to staff via a special site off the Legal Services website: http://chdintra.cdha.nshealth.ca/departmentservices/legalServices/index.html

**What is being asked of me as manager/ medical director in relation to *education*?**

* We need your help to make staff aware of the mandatory LMS course and to ensure it is done. We acknowledge this is a big task; however, we are required under *PHIA* to educate our staff, physicians and learners. Individuals who break the law could face fines up to 10,000 dollars or up to 6 months imprisonment and the organization can face fines up to 50,000 dollars!!! Two health employees in Newfoundland have recently been charged under their Act: <http://www.vocm.com/newsarticle.asp?mn=2&ID=33481>
* Email the FAQs for staff to those reporting to you
* We ask you to use the materials in this toolkit, via a staff meeting or another method you think best, to get staff talking about the new legislation, privacy protection at Capital Health, and consider various changes to your area or service that may need to be changed.

**What are the key changes for me in particular as a Manager/ Medical Director?**

* **Mandatory Privacy Breach Reporting:** All employees, physicians, learners, volunteers and other associates of Capital Health will be required to report privacy breaches to Capital Health by law. Employees are to report breaches using the patient safety reporting system and you will be required to investigate and assist in the resolution in accordance with Capital Health Privacy Breach Protocol, which is available on the Capital Health Internet site and as an appendix to the privacy policy.
* **Mandatory Patient Notification of Privacy Breaches:** In a case where a privacy breach causes a potential for harm and embarrassment, patients must be notified. Managers/Medical Directors will be responsible for doing the notification ordinarily, after consultation with the Privacy Officer. A decision not to notify must be agreed to by the Privacy Officer. It is anticipated provincial guidelines will be available soon. The Privacy Officer has a notification template letter.
* **User Access Auditing/Record of User Activity policy:** As part of *PHIA* implementation, there will be a new process in which managers and medical directors will potentially receive user access audit reports for their staff, either in response to a patient complaint or as part of our responsibility to proactively monitor staff for potentially unauthorized access. After receiving a report, managers and medical directors will have to determine whether the access was authorized or not based on whether the individual had a job related reason to access the personal health information. Patients may also request a record of everyone who looked at their personal health information on our electronic information systems and, you, as well as your staff, may be called upon to explain why it was necessary in your role. A draft proposed copy of the policy is included here, as we are awaiting provincial feedback.
* **Data minimization and De-identification:** Under *PHIA*, we must collect, use and disclose the minimum amount of personal health information to achieve the purpose, be it clinical care, research, teaching, quality, etc. For example, how much information do you need to request on a given form or include in a given database to achieve the purpose it was designed for? Personal health information must not be used if other information will achieve the purpose, e.g. Will the collection, use or disclosure of de-identified data achieve the purpose, such as de-identified case examples or statistics?
* **Limiting or revoking consent to collect, use, or disclose personal health information:** Under *PHIA*, individuals have the right to ask that personal health information not be collected, used or disclosed or to limit its use and disclosure, in cases where consent is required. For example, he/she could ask us not to give out personal health information to a specific health professional or organization. In response to a request, we are required to:
	+ Take reasonable steps to comply with the request. **Note:** There may be some cases where there is nothing we can reasonably do, especially given the interconnected nature of some of our electronic information systems and their inability to proactively block individuals from accessing specific patients. Some systems also have autofaxing, so it may be possible that the information has already been shared before the individual thinks to make the request.
	+ Advise them of any consequences of the request (e.g. patient safety concerns, continuity of care issues and access to care concerns, i.e. one of their health professionals may not feel confident that they have sufficient information to care for them).
	+ Advise a health care professional or organization when we are not releasing all the personal health information we feel is reasonably necessary because the individual has not provided us with consent to do so.

This process may make staff feel uncomfortable; however, such a notification can act as indication to the receiving health professional that there may be trust or other issues that they need to address, whereas before they might not have been aware of them as the patient could choose to withhold information without the health professional’s knowledge.

Given the breadth of different information systems and technologies that are used to share information within Capital Health and with those outside Capital Health, what is reasonable to do in response to a request will vary based on the nature of the request and the particular service. There is no system used at Capital Health at this time that we are aware of that can proactively block Capital Health staff with access to that system from seeing a patient record. Patients worried about internal staff access should be advised that:

1. staff are trained to only look at what they need to know;
2. some systems have audit logs and they can request a copy of who looked at their record from the Privacy Office, and
3. if the person with the concern feels comfortable, the manager of the particular area could inform the Manager of the Capital Health staff member they have concerns about to speak to them.

Managers should also think about how information gets disclosed in their area to other care providers outside Capital Health (e.g. what could you reasonably do if someone didn’t want their family physician, pharmacy, nursing home, etc. to know). If someone still does not want his or her personal health information to go to outside providers for care purposes after clinical staff have explained the risks, both the clinical staff member and the individual patient must fill out Capital Health’s Consent Directive form indicating the discussion has taken place and submit to it to Health Information Services. However, the patient should be aware it may be possible for an outside provider to the access the information through provincial or shared electronic information systems if that provider has access to them.

**What about research? Are there new rules governing the conduct of research under *PHIA*?**

Yes, *PHIA* addresses research and includes a legal definition of what constitutes research for the purposes of the Act. *PHIA* creates some new rules for research involving personal health information, in particular in sections 52-60 of the Act. Research Services will be updating its policies and forms to reflect *PHIA* requirements.

For information specific to research, please contact Mary Kate Needler, Program Manager –Research Quality, at 473-8549

**What are some key messages that staff, physicians, etc. need to know?**

We have developed some FAQS, which are attached as an appendix. We have also attached some news stories to raise awareness, along with some questions for discussion.

**How is Capital Health educating the public about these changes?**

* **Written Privacy Statement:** We are required by *PHIA* to have a written document in place that explains in general our information practices around personal health information, how to request a copy of their records and how to make complaint, among other information. We have answered these questions in the form of a patient education brochure that can be ordered (mid May) and it will be available on Capital Health’s privacy website for the public. It is attached here, as it is a good educational tool for staff as well.
* **Notice of Purposes Document:**  This document is modeled after the ones used by hospitals in Ontario and is intended to describe the common purposes for which we collect, use and disclose personal health information and what the patient’s rights are. **In particular**, we need to make it readily available to patients in order to rely on knowledgeable implied consent for the collection, use and disclose for **patient care purposes** and **teaching** (i.e. consent can be implied from the patient’s actions as the notice is likely to come to their attention and they did not refuse consent). We will need to post it in registration and admission areas, waiting areas, etc, as well as potentially including it in appointment letters. It too will be important for staff to be familiar with, as patients may have questions for them based on it and staff are required to assist the individual if they believe an individual has a limited ability to read it or comprehend the information, whether due to a disability, limited reading ability, language considerations, etc. Your staff should be engaged to identify areas or ways to bring this to individual’s attention and post it. If you currently obtain express consent in your area upon admission to personal health information collection, use and disclosure, you may continue to do so but the information in the notice of purposes must be covered in your express consent process at a minimum. Express consent forms should be reviewed for *PHIA* compliance with Legal Services.
* **Public website:**  The above two documents, as well as other forms and documents, will be available to the public on Capital’s Health Privacywebsite: <http://www.cdha.nshealth.ca/privacy-confidentiality>
1. **FAQS for Capital Health Staff, Physicians, Learners, etc. about Privacy and the *Personal Health Information Act (PHIA)***

**What is the *PHIA*? When** **is it law?**

On June 1, 2013, the *Personal Health Information Act* *(PHIA)* and its regulations will be law in Nova Scotia. Like health privacy legislation in other Canadian provinces, it governs the collection, use, disclosure, retention, disposal and destruction of personal health information at Capital Health. There are a number of new requirements and changes that affect how we manage personal health information at Capital Health. These changes will impact direct clinical care, teaching, research and quality improvement activities at Capital Health, amongst others.

**What educational tools will be provided to me?**

**You should complete the mandatory Privacy and Confidentiality LMS Course and survey question as soon as possible**. It is available now on the CDHA LMS site: <http://lms.cdha.nshealth.ca>  **.** Full step by step instructions are included at the end of this FAQs document.

**NOTE: You must complete the course before you are allowed to do the survey question.**

 Individuals who do not complete it in a timely manner may have their access to systems containing personal health information suspended. Your manager/ medical director will communicate with you with more details around how to complete the course, as it is possible to do it individually or as part of a classroom session.

Updated privacy and release of information policies will be in place in late May, as well as policies and procedures around the conduct of research. There will also be a new user accessing auditing policy. In addition, information sessions /lunch and learns with Capital Health’s Privacy Officer will be held at a variety of sites in May and are open to everyone. Some areas have already received presentations at the area’s request.

**How does *PHIA* define Personal Health information?**

Personal health information is individually identifiable information, or information that could reasonably lead to the identification of an individual, and includes, but is not limited to:

* demographic and registration information, such as name, date of birth, address and phone number, health care provider identity, health card number, substitute decision maker identity
* physical and mental health care history, including health history of the individual’s family
* information related to payments or eligibility for healthcare
* Information related to the application, assessment and provision of healthcare
* Relates to the donation of body parts or substances

Personal health information can be recorded or unrecorded, such as a printed lab result or a verbal conversation, and continues to be protected after death.

**Who is the custodian of personal health information at Capital Health?**

Although this has always been the case, *PHIA* legally confirms that CDHA is the custodian of personal health information collected from patients who receive care within CDHA facilities. A custodian is an organization or individual who has custody or control of the personal health information, as a result of performing their powers or duties and types of custodians are listed specifically in the PHIA and its regulations. Individual employees, clinicians and services are not custodians, but rather agents of CDHA under the law. Agents are persons who are authorized by the custodian to act for or on behalf of the custodian, for the custodian’s purposes and not the agent’s purposes. As agents, you do not have the right to collect, use or disclose personal heath information except as permitted by CDHA and in compliance with the requirements of *PHIA*. For example, a physiotherapist who works part time at Capital Health and then runs her own private clinic would be an agent of Capital Health while providing Capital Health registered clients with services at Capital Health. She would be the custodian of the personal health information of clients who seek her services in her private clinic.

**My patient asked for his lab results or a copy of a record from his chart. Can I provide it?**

*PHIA* permits us to tell patients information from their health record or give them a copy of a specific document or portions of the record upon their request. Accordingly, where appropriate clinically, Capital Health physicians and staff can provide information to patients from their health record. If the patient is seeking records to give to a care provider outside of Capital Health for the purpose of ongoing care, the outside care provider can contact Health Information Services to get the information as well. If the individual is seeking copies of his records for his own or for third party use (i.e. insurance companies, lawyers, Worker’s Compensation Board, etc) and the request involves a significant amount of records or records you do not have, individuals should be referred to our Access to Personal Health Information team (473-5512), which handles these types of third parties requests to for all of Capital Health.

**The patient’s sister wants to know his lab results over the phone or asks to view documents from his chart. Can I provide it to her?**

If the patient lacks capacity and the sister is the patient’s substitute decision maker, then the information can be shared. Otherwise, the patient must expressly consent to the sister receiving this health information. In terms of general information, *PHIA* allows us to share with family and friends confirmation a patient is in hospital, his or her room and telephone extension, and general condition (e.g. good, fair) on the day they ask, unless the patient has objected. To share any additional personal health information beyond this general information requires the express consent of the patient.

**Can I look up my own record either directly or by giving permission to another co-worker? Can I look up family, friends or co-workers if they ask?**

No. You are only authorized to look up individuals who are under your direct care or that you need to as part of your official duties at Capital Heath, aka “the need to know principle.” Looking up individuals you are not authorized to by Capital Health is a breach of privacy, even if they give their consent. For example, your friend or co-worker consents to you telling her test result, but you are not part of the care team or qualified to explain the result. Individuals seeking personal health information should contact their care team or other CDHA authorized staff who release health records. You are only authorized to view your own personal health information in the custody or control of Capital Health through the method approved for the public in the CDHA *Release of information from the Health Record* policy. You can call our Access to Personal Health Information team at 473-5512 for more information.

**You mentioned a new user access auditing policy earlier? How will that process work?**

Audit systems are in place to track what personal health information you view on Capital Health electronic information systems. In addition to reviewing your access if an individual raises a particular access concern, we will also be actively monitoring user access for potential incidents of unauthorized access. Your manager or medical director may be sent a report about your access and you may be asked to explain why you accessed the information. In addition, you should be aware that under *PHIA*, any individual has the legal right to obtain a list of everyone who looked at their personal health information on our electronic information systems free of charge. This may also lead to questions from individuals about whether your access was authorized or not.

**If I suspect a privacy breach has occurred, am I required to report it to Capital Health? Do patients have to be told?**

As an agent of Capital Health, you are required by law under PHIA to report any loss, theft or unauthorized access to personal health information at the first reasonable opportunity. Reports should be made to your manager or Medical Director and the Capital Health Privacy Office using the Patient Safety Reporting system and in accordance with Capital Health’s Privacy Breach Protocol, located on Capital Health’s Privacy internet site. In a case where a privacy breach causes a potential for harm and embarrassment, patients must be notified under *PHIA*. It is anticipated provincial guidelines will be available about patient notification soon.

**What are some general principles that apply to how we handle personal health information?**

* **Data minimization and De-identification:** Under *PHIA*, we must collect, use and disclose the minimum amount of personal health information to achieve the purpose, be it clinical care, research, teaching, quality, etc. For example, how much information do you need to request on a given form or include in a given database to achieve the purpose it was designed for. Personal health information must not be used if other information will achieve the purpose, e.g. Will the collection, use or disclosure of de-identified data achieve the purpose, such as de-identified case examples or statistics.
* **Need to Know:**  We can only share personal health information with others who are authorized to receive the information. As mentioned above, you are only authorized to access the personal health information of individuals who are under your direct care or that you need to as part of your official duties at Capital Heath. Discussing personal health information with individuals within or outside of Capital Health who do not need to know the information is a breach of patient privacy.

**What are the consent rules around the collection, use and disclosure of personal health information for different purposes?**

Depending on the purpose of the particular collection, use or disclosure, one of the following consent rules will apply:

(a) consent may be implied from the individual’s actions,

(b) express written or verbal consent is required, or

(c) no consent may be required.

Some examples of each type of situation follow:

***Knowledgeable implied consent***

We can collect, use and give out personal health information for the **purpose of patient care** based on the principle of “knowledgeable implied consent.” This principle requires us to provide patients with sufficient information around why we collect use and disclose personal health information and his/her right to give or withhold consent, either through a readily available poster/brochure or a discussion. Having done so, Capital Health can then rely on this consent to share personal health information internally with staff who need to know it to either directly provide or support care. For example, when a patient enters an emergency waiting area, posters describing the common uses and disclosures we make for care purposes, amongst others, will be readily available. If a patient decides to seek care from us, having had the opportunity to read the poster, we can assume he or she is consenting to having his or her personal health information shared with the appropriate Capital Health staff and associates, such as physicians, pharmacists, medical lab technicians, dieticians or ward clerks, in order to care for him or her. We can also disclose it to other health professionals outside our organization in order to help them provide care, unless the patient objects. This standard also applies to **our teaching activities.**

However, if it comes to Capital Health staff’s attention that an individual has a disability or limited ability to read or understand the notice or the language it is written in, staff must make reasonable efforts to assist in explaining the information or obtain help from Language and Interpretation Services.

***Express consent***

Some examples of when we must obtain express consent include:

* Disclosing personal health information to non custodians, unless required by law;
* Disclosing personal health information to the media, fundraising bodies, or marketers;
* Using or disclosing personal health information as part of research studies. Note: Some research studies do not require consent and have safe guards in place, such as Research Ethics Board review and approval.
* Giving insurance companies, employers or the individual’s legal counsel access to his/her health record;
* Disclosing anything other than general information, i.e. the fact the individual is a patient, location, and general condition (e.g. stable) to your family and close friends, on the day they ask.

***No consent required***

In certain situations we are permitted or required to collect, use and disclose personal health information without consent, including, but not limited to:

* Billing provincial health plans
* Responding to a court order
* Plan and manage our internal operations
* Conduct quality improvement and risk management activities, e.g. patient safety reporting
* Enable the Department of Health and Wellness to plan and manage the health care system

The most important ones will be summarized in the privacy policy (collection and use rules) and release of information policy (disclosure rules).

**Can individuals limit or withdraw their consent personal health information?**

Under *PHIA*, individuals have the right to ask that personal health information not be collected, used or disclosed or to limit its use and disclosure, in cases where consent is required. For example, he/she could ask us not to give out personal health information to a specific health professional or organization. In response to a request, we are required to:

* Take reasonable steps to comply with the request
* Advise them of any consequences of the request (e.g. the lack of information may result in an adverse event with their care or one of their health professionals may not feel confident that they have sufficient information to care for them).
* Advise a health care professional or organization when we are not releasing all the personal health information we feel is reasonably necessary because the individual has not provided us with consent to do so.

This process may make you feel uncomfortable; however, notifying the receiving health professional of a request that you feel will have an impact on care may actually help the patient – provider relationship in some cases. The health professional will know that there may be trust or other issues that they need to address, whereas before they might not have been aware, in some situations the patient could choose to withhold information without the health professional’s knowledge.

**What can I or my service area reasonably do in response to a request?**

What you can reasonably do varies depending on the nature of the request and the nature of the service. Currently, patients who want to keep outside callers from being able to confirm they are a patient can do so by telling staff working in the area upon admission. They can also tell staff that they do not want a student to observe a procedure. Patients worried about Capital Health staff access should be advised that:

1. staff are trained to only look at what they need to know;
2. some systems have audit logs and they can request a copy of who looked at their record from the Privacy Office, and
3. if the individual feels comfortable, the manager of the particular area could inform the Manager of the Capital Health staff member they have concerns about to speak to them.

If someone still does not want his or her personal health information to go outside providers for care purposes after clinical staff have explained the risks, both the clinical staff member and the individual patient must fill out Capital Health’s Consent Directive form indicating the discussion has taken place and submit to it to Health Information Services and the Privacy Office. However, the patient should be aware it may be possible for an outside provider to the access the information through provincial or shared electronic information systems if that provider has access to them. When faced with particular request, consult with your manager and the Privacy Office if you are unsure how to respond. Document the request and actions taken on the patient chart.

**Who can I disclose information to under *PHIA* and for what purpose?**

Refer to Capital Health’s *Release of information from the Health Record (CH-30-015)* for the most common situations. If you experience a situation not covered in the policy, contact your manager or the Privacy Officer.

**Are there other policies in relation to privacy, security and confidentiality of personal health information I should be aware of?**

Below is a list of some key ones as of May 1, 2013. The list, while not exhaustive, is intended to act as a quick reference guide for staff with questions about what policies currently exist. This list will be updated from time to time on Capital Health’s privacy website. Certain policies, such as the privacy policy and release of information policy, will be updated in time for June 1st, 2013.

|  |  |
| --- | --- |
| **Core Privacy, Confidentiality and Security of Patient Health Information Policies**  | **Policy Number** |
| Privacy | CH 100-100 |
| Release of Information from the Health Record | CH30-015 |
| Release of information Restriction –Verbal Communications Black out | CH30-014 |
| Security of Health Information during Transport  | CH30-061 |
| Confidential Waste Management | CH90-015 |
| Administration of Research | CDHA RS 01-001 |
| Retention of Records | CH100-055 |
| Retention of Research Records | CDHA RS 01-011 |
| Computer Password | CH 50-015 |
| Computer End User Acceptable Use | CH 50-020 |
| Internet Access/Use | CH 50-005 |
| Acceptable Encryption | CH 50-040 |
| Email Acceptable Use | CH 50-045 |
| Remote Access | CH 50-070 |
| Interacting with Law Enforcement Agencies | CH 100-065 |
| Media Relations | CH 70-025 |
| eHealth Information Technology Audit | CH05-010 |

**What about research? Are there new rules governing the conduct of research under *PHIA*?**

Yes, *PHIA* addresses research and creates some new rules for research involving personal health information. Research Services will be updating its policies and forms to reflect *PHIA* requirements.

For information specific to research, please contact Mary Kate Needler, Program Manager –Research Quality, at 473-8549

**What are the consequences if I breach patient privacy, my confidentiality agreement or responsibilities in other related policies?**

A breach may result in corrective action, up to and including significant disciplinary action. Action taken may include, but is not limited to: retraining, loss of access to systems, suspension, reporting my conduct to a professional regulatory body or sponsoring agency, restriction or revocation of privileges, and immediate dismissal. A breach under PHIA may lead to prosecution by the Nova Scotia Government. Penalties can include fines for individuals up to 10,000 dollars or up to six months imprisonment. A civil suit may also be brought against me by the party harmed. The provincial privacy officer may conduct a review as well.

**Instructions for accessing LMS Privacy and Confidentiality course**

The MANDATORY Privacy and Confidentiality LMS Course is now available on the **CDHA e-learning website,**

<http://lms.cdha.nshealth.ca>

On this site each user will have to **complete two things**: the course (which includes a 6-question quiz at the end), and a survey question which affirms and updates your confidentiality pledge. You must complete the course before you can complete the survey.

This is how to access the course and survey question.

Go to the main page of intranet <http://chdintra.cdha.nshealth.ca/>

1. Go to the main page of intranet <http://chdintra.cdha.nshealth.ca/> and in the right hand colum under **Quick Links** click on **LMS** OR go to <http://lms.cdha.nshealth.ca>
2. Click the **LMS Icon (in purple)** at right hand side of page **Click Sign In** on the upper left corner.
3. Once you have clicked the LMS button you will proceed to the sign in page. Click **Sign In**, in the top right corner.
4. **Enter your username and password to sign in:**

**Username:** **Employee # (found on paystub)**

Password: **Employee #**

1. You will then proceed to the following page, on this page click the **catalogue button** to select a course you wish to take
2. Once you have clicked the catalogue button you will proceed to the following page: On this page you can scroll down the page to see courses that are available or type **Privacy and Confidentiality** in the search box or in the ‘all catalogues’ dropdown menu, find **PRIVACY AND CONFIDENTIALITY. Click GO.**

On the first line, you will see the Survey, which will be done after you complete the course

[**Survey Prov-DHA-IWK-Aff-2013v1: Pledge of Confidentiality ReAffirmation**](https://elearning.nshealth.ca/HITSNS-shared/LearningStudio/index.cfm?fuseAction=MyLearningCenter.LandingPage&tab=&ItemId=753)

On the second line you will find the link to the course**. Do this course first.**

[**Course Prov-PC-2013v1: Provincial DHA/IWK Privacy and Confidentiality Training**](https://elearning.nshealth.ca/HITSNS-shared/LearningStudio/index.cfm?fuseAction=MyLearningCenter.LandingPage&tab=&ItemId=714)

1. On both lines, click **SELECT THIS ITEM**. It will ask you to **ADD to MY LEARNING**. **You will get a popup box that says ADD THIS COURSE TO MY COURSES (OR SURVEYS).**
2. You will see a tab that says **MY LEARNING** and these two items will appear. Begin the course, which will take less than 15 minutes.

\*Near the end of the course, you will be asked to reread the confidentiality pledge, which can accessed by clicking on the “attachments” tab. This means a file has to be downloaded on your computer. A new window will pop up and may ask you if you would like to allow this file to download. Say yes. Once you read the pledge, close the window.

1. Once you finish the course, **you need to go back to MY LEARNING, select and complete the survey**. Click on it. It takes less than one minute to complete.
2. Click **SIGN OUT** on the upper left corner and congratulations, you are finished!
3. **CAPITAL HEALTH PLEDGE OF CONFIDENTIALITY**



**PLEDGE OF CONFIDENTIALITY**

I pledge to keep confidential any information obtained during the performance of my duties at Capital Health, whether as an employee or an associate[[1]](#footnote-1). I understand that confidential information includes, but is not limited to, information relating to:

* Patients (such as health records, conversations, registration information, financial history, etc.);
* Capital Health employees and other associates (such as employee records, disciplinary action, etc.);
* Capital Health business information (such as contracts, memos, peer review information, etc.).

I agree that I will read and comply with Capital Health’s policies on privacy, confidentiality and security of confidential information. If I require help in retrieving or understanding these policies, I will seek help from my manager or Capital Health’s Privacy Office.

I also understand and agree that:

* I will collect, access, use and disclose confidential information on a “need to know basis” only, and only the minimum amount required, as required for my role or as required by law. I will not communicate confidential information either within or outside Capital Health, except to persons authorized to receive such information.
* I will not access the confidential information of family, friends, co-workers or any other individual, unless they are under my direct care or I need to as part of my official duties at Capital Heath.
* I will access my own personal health information in the custody or control of Capital Health through the method approved for the public in the *Release of information from the Health Record* policy.
* I will not share my passwords to electronic information systems with anyone and I am responsible for protecting them. I am responsible for all actions performed when the electronic information system has been opened using my password.
* I will access, process and transmit confidential information using only authorized hardware, software, or other authorized equipment.
* I shall not remove confidential information from Capital Health premises except as authorized. In transit, I shall securely store the information and ensure it is in my custody and control at all times.
* I will not alter, destroy, copy or interfere with confidential information, except with authorization and in accordance with Capital Health policies and procedures;
* I shall immediately report all incidents involving loss, theft or unauthorized access to confidential information to my immediate supervisor and to Capital Health’s Privacy Office.
* I understand that the Capital Health will conduct regular audits to ensure confidential information is protected against unauthorized access, use, disclosure, copying, modification or disposal.

I further understand any breach of my duty to maintain confidentiality may result in corrective action, up to and including significant disciplinary action. Action taken may include, but is not limited to: retraining, loss of access to systems, suspension, reporting my conduct to a professional regulatory body or sponsoring agency, restriction or revocation of privileges, and immediate dismissal.

I understand and agree to abide by the conditions outlined in this agreement, and they will remain in force even if I cease to be employed by or have an association with Capital Health.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Employee/Student/Volunteer /Associate

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Witness

1. **GROUP EDUCATION/DISCUSSION PRIVACY MATERIALS**

Have your staff read the following 3 newspaper articles and ask them the following questions:

1. Do you believe there is a culture of “everyone does it” at Capital Health? If so, how can we best change the culture?
2. What do you think are the biggest privacy risks in your work area? How can you help address them? What can the organization do?
3. What harm can be experienced by patients and the health care system as a whole as a consequence of a privacy breach?
4. Did you ever discover a privacy breach? Did you report it?
5. Have you ever disclosed a privacy breach to a patient? What was it like?
6. How important is privacy and confidentiality to your relationship with patients?
7. If you received a record of everyone who looked at your health information on Capital Health, how would you feel if you recognized a neighbor, a co-worker, etc, who wasn’t a part of your care?

## Article 1: St. Albert doctor suspended for privacy breach, St Albert Gazette, Mar 28, 2013

<http://www.stalbertgazette.com/article/20130328/SAG0801/303289997/-1/sag0801/st-albert-doctor-suspended-for-privacy-breach>

An emergency room doctor from St. Albert has been suspended for at least a month because she illegally tapped into restricted medical files.

The College of Physicians & Surgeons of Alberta announced this week that it had found Deanne “Dee” Gayle Watrich, an emergency room doctor and a St. Albert resident, to be guilty of unprofessional conduct.

Watrich had previously admitted to unprofessional conduct at a hearing tribunal held by the college last November.

Specifically, the tribunal wrote in its ruling, Watrich accessed the electronic health records of three people 21 times between Aug. 5, 2009, and May 2, 2010, without having a patient/physician relationship with those people.

It’s okay for doctors to access patient records if they are actually treating those patients, explained college spokesperson Kelly Eby, but not otherwise.

“She accessed the electronic health records of three people who she was not treating,” she said. “It’s an invasion of privacy.” It also violates the provincial Health Professions Act and Health Information Act, and goes against the Canadian Medical Association’s Code of Ethics and the college’s standards of practice.

Watrich’s case started when the provincial privacy commission began investigating a complaint from a man who had requested an Alberta Netcare log. The log showed that nine doctors, none of whom were treating him, had accessed his electronic health records. He alleged that Watrich might be the one responsible.

The man listed his partner and mother as co-complainants, both of whom had their files accessed by three other doctors.

Watrich admitted to the privacy commissioner and to the tribunal that she was responsible for accessing these restricted records using the logins of 12 other doctors.

On 21 occasions, the tribunal heard, Watrich used computers in the emergency department of the Edmonton Misericordia Hospital to access these records after the previous user had not logged out, and did so knowing that her personal ID would not show up in the computer’s logs as a result.

Watrich was in a personal relationship with one of the complainants when she accessed some of the records, the tribunal found, and in a relationship with the former spouse of said complainant when she accessed others.

“I don’t know why I logged in to their Netcare and why I did it so many times,” Watrich said at the hearing last November. “It didn’t actually give me any power. It didn't give me anything.” In retrospect, she believed accessing these records might have been a way for her to cope with the difficult divorce and child-custody proceedings her partner was going through at the time.

Watrich told the tribunal that she was humiliated and embarrassed by her actions and “deeply disappointed in (herself).” She had apologized to the complainants, and paid a “significant monetary settlement” to them in a related lawsuit. Covenant Health (which runs the Misericordia) had also put a reprimand on her record.

Even though Watrich didn’t disclose any of the information she accessed, the tribunal ruled, her actions were done repeatedly and with intent to deceive, and impugned the reputation of her fellow physicians.

The tribunal suspended Watrich from medical practice for 60 days. She will be actively banned for 30 days and then on probation for six months, during which she may be suspended for another 30 days if she does not show good behaviour.

Watrich was also ordered to take an ethics course and to pay $22,232.59 to cover the cost of the college’s investigation. She has done both.

The tribunal’s ruling can be found at cpsa.ab.ca

# Article 2: Report slams snooping by Regina health-care workers, CBC NEWS, Feb 13, 2013 <http://www.cbc.ca/news/canada/saskatchewan/story/2013/02/12/sk-health-care-privacy-1302.html>

*Gary Dickson, Saskatchewan's information and privacy commissioner, wants stricter rules to deal with how health-care employees access private records.* *(CBC)*

Several Regina-area health care workers have been snooping into their co-workers' confidential medical records and in one case altered the records to add "RIP," Saskatchewan's privacy commissioner says.

Gary Dickson said his office investigated three disturbing cases from 2008 to 2010 where workers covered by the Regina Qu'Appelle Health Authority improperly accessed the health records of other workers.

In one case, an employee at the Regina General Hospital heard that a co-worker had been receiving health services. She looked up the co-worker's records and displayed them on a computer screen while other workers looked over her shoulder.

At the time, no one present suggested there might be something wrong with that, although the worker later confessed to the co-worker.

**'Unauthorized viewing of personal health information involving electronic information systems at [the health region] was becoming a chronic issue.'***—Gary Dickson, Saskatchewan privacy commissioner*

In a second case, when a lab employee went into her own medical information, she found that someone had altered her electronic records.

"She discovered that her name, sex, and infectious disease information ... had been changed. Her name was replaced with vulgarities and the acronym 'RIP' appeared in her file," the privacy commissioner's report said.

It was later found that another employee in the health authority had accessed her records seven times.

The third case involved an employee whose husband was involved in a custody dispute with his ex — who also worked in the health region.

The ex accessed the employee's medical records for reasons the health regions said "appear to be intentional, malicious and for personal gain."

The cases resulted in suspensions and other disciplinary measures.

In the Regina General Hospital case, a worker was fired, but she was later rehired after a labour arbitration. In the "RIP" case, the employee identified as the culprit was terminated. In the third case, the employee was suspended for 20 days.

Dickson said the three cases seem to point to a widespread problem.

"It appeared to my office that perhaps the unauthorized viewing of personal health information involving electronic information systems at [the health region] was becoming a chronic issue," the report said.

Dickson also said the health authority was generally proactive in looking into the complaints, although it didn't clamp down on what was going on even after being alerted about the first case in 2009.

**'Everybody does it', worker says**

It appeared there was a culture of "everybody does it" that seemed to be at work in the health region, the report said.

*Diane Aldridge, director of compliance for the Saskatchewan privacy commissioner, says unauthorized snooping erodes confidence in the health system. (Stefani Langenegger/CBC)*

Diane Aldridge, director of compliance for Dickson's office, noted Tuesday that workers who nose around in confidential files could face serious consequences whether or not their intentions are malicious.

"Why they're accessing the information isn't really that important," Aldridge told CBC News. "It's about patient confidence, not only in the electronic health record but in the system itself."

Aldridge echoed Dickson's observation that the breaches seemed to be commonplace, according to their investigation.

"[An] employee was asked why she looked at the information [and] she said it was curiosity and boredom and everybody does it," Aldridge said.

Dickson is calling for action to make the system more secure and to stop employees from repeating these kinds of intrusions.

For example, health-care workers who log on to a computer and access medical records shouldn't just walk away when they're done, he says — they must log off so no one else can get into secure areas.

# Article 3: Massive breach at 2nd Newfoundland health authority, CBC NEWS, Aug 1, 2012

# <http://www.cbc.ca/news/canada/newfoundland-labrador/story/2012/08/01/nl-western-health-privacy-801.html>

The health authority in western Newfoundland said Wednesday it fired an employee for accessing the medical records of more than 1,000 patients, just a week after similar privacy breaches were disclosed in St. John's.

Western Health said it is now contacting 1,043 patients whose records were accessed by a single employee, and will be apologizing to each one.

"Privacy breaches such as this one are extremely unfortunate," chief executive officer Dr. Susan Gillam said in a statement.

It's not clear how Western Health discovered the breach, although the authority said that it conducts audits of how employees access patient records.

Gillam said Western Health has a zero tolerance policy on information breaches.

The disclosure comes just a week after St. John's-based Eastern Health, the largest authority in Newfoundland and Labrador, reported that it had fired five employees for similar breaches, and had suspended six others.

As with Eastern Health, employees at Western Health are required to take a confidentiality pledge, and not access the records of patients who fall outside what is called their circle of care.

"We take our responsibility as the custodians of an individual’s personal health information very seriously and with the utmost care and concern," Gillam said.

Ed Ring, Newfoundland and Labrador's privacy commissioner, said he is concerned about such incidents, but said the health authorities are doing what they can to prevent breaches.

"I think they have good policies, they have a great privacy team, but it doesn't matter how good the rules and the policies and procedures are," Ring told CBC News.

"If somebody with wilful intent is going to break the rules, then it's pretty hard to stop that."

Last week, Colleen Weeks, a nurse who was fired from a St. John's hospital, told CBC News that she had done nothing wrong, and that many other employees did the same thing.

While Weeks said she was concerned about the health of others, the letter sent to her by Eastern Health said she had, among other things, accessed records of her ex-husband, a tenant and her boyfriend's former partner.

# Article 4: My ex's wife snooped into my health records, woman says, CBC NEWS, Aug 23, 2012

<http://www.cbc.ca/news/canada/newfoundland-labrador/story/2012/08/23/nl-central-health-privacy-lawsuit-823.html>

A St. John's woman is the latest to file a lawsuit against a regional health authority over a privacy breach, and says the violation was deliberate and personal.

Shawna Thompson says her ex-husband's wife inappropriately accessed her medical records, including lab test results and other confidential information that had been held at Central Health.

"I'm very angry and I'm outraged," said Thompson, who is the complainant in a lawsuit brought by St. John's lawyer Bob Buckingham against Central Health.

"I know she shared it with my children, so that would give me an idea that she has probably shared it with a lot of people."

Thompson said Central Health didn't do enough to protect her, as her files were viewed by the same person 22 times in the past seven years.

The suit is the third that Buckingham has brought against health authorities over the last week. He is leading class action suits against Western and Eastern Health, in the wake of a series of privacy breaches that became public this summer.

Central Health has reported several privacy breaches within the last year and a half. In March 2011, [the authority fired an employee](http://www.cbc.ca/news/canada/newfoundland-labrador/story/2011/03/07/nl-central-breach-307.html) for accessing the files of 19 patients.

But this July, the authority [admitted it had had two other recent breaches](http://www.cbc.ca/news/health/story/2012/08/02/nl-more-privacy-breaches-802.html) that it had not previously reported, and disclosed them only after CBC News followed up on similar breaches at other authorities. In one case, an employee was suspended, and in the other, the employee resigned.

Although the authority has promised to tighten up its privacy protocols, Thompson — who had obtained health services in years past from Central Health staff — is seeking redress in the courts.

"There's all kinds of issues Central Health should look at and probably have since this started," said Thompson. "But at this point in time now, the damage is already done for me."

Thompson, who said she has been traumatized by the experiences, said she has had trouble sleeping since finding out her records were accessed without her knowledge, but is afraid to consult a doctor over fears for her privacy.

Central Health informed Thompson of the breach last November.

**[CBC Poll done as part of the story]**

**A third health board in N.L. has been served with a lawsuit over patient privacy breaches by staff. What do you make of this?**

Some health care workers still think there's nothing wrong with looking up medical information about people they know  35.12%  (583 votes)

Health authorities have not made their privacy policies clear enough to employees  13.92%  (231 votes)

Health authorities have to do more to keep their workers away from confidential information  41.45%  (688 votes)

Everyone knows everyone else in N.L. - there is no such thing as privacy anywhere in this province  10%  (158 votes)

Total Votes: 1,660

|  |  |  |  |
| --- | --- | --- | --- |
|  | Auditing of Access to Personal Health Information (PHI) in Electronic Information Systems and Record of User Activity Requests | NUMBER: DRAFT –V.4 |  |
| Effective Date:  |  | Page | (1 of 7) |
| Applies To: | Holders of the Capital Health Administrative Manual |

##### **CAPITAL HEALTH DRAFT USER ACCESS AUDITING POLICY**

##### POLICY

1. To ensure patients disclose information needed to provide safe patient care, Capital Health must maintain public trust that the information patients provide is only accessed for authorized purposes. Capital Health is committed to ensuring that personal health information (PHI) in its custody or control is protected against unauthorized or inappropriate access and has a responsibility to implement reasonable safeguards to preserve the confidentiality of that information.
2. Capital Health recognizes the importance of auditing user access to personal health information in electronic information systems as a mechanism to help detect and deter unauthorized access. The objectives of this Policy are to:
	1. Communicate Capital Health audit requirements, processes and accountabilities to all users of Capital Health electronic information systems containing personal health information.
	2. Mandate appropriate audit controls and mechanisms to help protect patient information from unauthorized access; and
	3. Support a privacy conscious environment within Capital Health.

##### Scope

* 1. This Policy applies to any access to personal health information contained in any electronic information system for which Capital Health is the custodian, including, but not limited to the detailed list of programs, services and individuals contained in the scope of Capital Health’s *Privacy* Policy (CH100-100).
		1. In addition, this Policy applies to all users granted access to Capital Health electronic information systems containing personal health information.

##### Compliance

* 1. It is the collective responsibility of all users to comply with the Privacy Audit Programs as described in this Policy.
	2. Any breach of this Policy may result in disciplinary consequences up to and including termination of employment or services, in accordance with Capital Health’s *Corrective Action* Policy (CH40-045), and for physicians, may include loss of privileges in accordance with Medical Staff Bylaws and Rules.

DEFINITIONS

|  |  |
| --- | --- |
| **Agent:**   | In relation to a custodian, means a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not for the agent’s purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian, and includes, but is not limited to, an employee of a custodian or a volunteer who deals with personal health information, a custodian’s insurer, a lawyer retained by the custodian’s insurer or a liability protection provider. (*Personal Health Information Act*, s. 3(a)) |
| **Audit:**   | A review or examination of logged events within an electronic information system. |
| **Audit log:** | An electronic record/file of events recorded by an electronic information system, which generally details who accessed personal health information in the system during a given time period and what activities were performed.  |
| **Audit plan:** | A written plan that defines which electronic information systems will be audited and the types of audits that will be conducted (e.g. behavior specific audits (e.g. co-worker/neighbor viewing), random audits, user role/service area specific audits, etc). The plan includes a schedule of when audits will be run (i.e. monthly, quarterly, etc.). |
| **Custodian:**   | An Individual or organization listed in the *Personal Health Information Act* and its regulations, who has custody or control of personal health information as a result or in connection with performing the person’s or organization’s powers or duties. (*Personal Health Information Act*, s. 3(f)). For the purposes of this policy, the custodian is Capital District Health Authority. |
| **Electronic Information System:** | A computer system that generates, sends, receives stores or otherwise processes personal health information. |
| **Incident-based Auditing Program**: | A program for staff, patients and others to report potential unauthorized or inappropriate access to electronic information systems containing personal health information to the Capital Health Privacy Officer for investigation. The program involves the retroactive review of audit logs for evidence of inappropriate or unauthorized access.  |
|  |  |
| **Personal Health Information:** | Identifying information about an individual, whether living or deceased, and in both recorded and unrecorded forms, that relates to:1. the physical or mental health of an individual, including information that relates to the health history of the individual’s family,
2. the application, assessment, eligibility and provision of healthcare to the individual, including the identification of a person as a provider of health care to the individual,
3. payments or eligibility for health care in respect of the individual,
4. the donation by the individual of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance,
5. the individual’s registration information, including the individual’s health card number,
6. the identification of an individual’s substitute decision maker.
 |
| **Proactive Auditing Program**: | A program (absent any report or compliant submitted to the Capital Health Privacy Officer) that involves the proactive review of audit logs for patterns indicating possible unauthorized or inappropriate access to personal health information. The program may include a review of randomly selected users, patients or events or a review based on scenarios which are commonly held to indicate a higher risk of unauthorized access. |
| **Record of User Activity:** | A report produced at the request of an individual for a list of all users who accessed an individual’s PHI on an electronic information system for a time period specified by the individual. It is generally derived from the electronic information system’s audit log. (See Appendix A for the legal minimum requirements for a record of user activity.) |
| **Unauthorized Access:** | Access to personal health information that is not required to carry out a user’s duties and responsibilities, as defined by Capital Health. Unauthorized access includes, but is not limited to, accesses by a user to:1. their own personal health information ,
2. a co-worker’s personal health information, unless necessary to do his/her job,
3. the personal health information of family, friends, neighbors or other individuals known or unknown to the individual, unless necessary to do his/her job.
 |
| **User:** | Any person accessing CDHA electronic information systems containing personal health information. |

**GUIDING PRINCIPLES AND VALUES**

1. Respect for the right of individuals to privacy, within the limits of the law, and the duty of confidentiality are essential to maintaining trust within the client care or service provider relationship.
2. Accountability and transparency to the public regarding access to personal health information in our custody and control.
3. Auditing resources should be allocated strategically using a risk based approach.
4. Capital Health auditing methods and processes should take into account applicable best practices and must comply with the relevant privacy legislation, other applicable laws and provincial policies.

**PROCEDURE**

1. **Responsibilities and Accountabilities**
	1. **All Users**:
		1. Comply with the terms of use and policies applicable to the use of electronic information systems containing personal health information;
		2. Report suspected unauthorized or inappropriate access to electronic information systems containing personal health information by others in accordance with this Policy;
		3. Cooperate with investigations and collaborate with management and the Privacy Officer to prevent reoccurrences.
	2. **Leadershift Enabling Team (LET)**:
		1. Supports and resources educational and technological initiatives related to the implementation and ongoing maintenance of Capital Health’s Privacy Audit Program, to the extent reasonable to achieve the organization’s acceptable level of risk.
	3. **Capital Health** **Privacy Office**:
		1. Maintains and administers this Policy;
		2. Coordinates and/or conducts the initial investigation of potential and actual privacy breaches brought to its attention through Capital Health’s Privacy Audit Program;
		3. Assists Human Resources, Managers/Supervisors, Medical Directors and Department Heads as needed to investigate privacy breaches;
		4. Runs audit reports to distribute to Managers/Medical Directors;
		5. Provides education with respect to Capital Health’s Privacy Audit Program;
		6. Ensures reporting of actual breaches of privacy in accordance with Capital Health breach guidelines, including but not limited to: the individuals affected, Nova Scotia’s Privacy Review Officer, Department of Health and Wellness and Capital Health Media Relations and members of the LET, as appropriate;
		7. Liaises with the Nova Scotia Privacy Review Officer, as appropriate;
		8. Notifies or makes recommendations to notify affected individuals, as appropriate, after consultation with Manager/Medical Director;
		9. Makes recommendations on disciplinary action, as appropriate.
	4. **Managers/Supervisors**
		1. Ensure staff members are aware of this Policy and Capital Health’s Privacy Audit Program;
		2. Conduct appropriate investigations into the facts surrounding user access in an individual case, as required by the Privacy Audit Program;
		3. Determine, in consultation with the Privacy Officer and Human Resources (HR), whether an access to electronic information systems by staff is authorized and appropriate;
		4. Work with HR to ensure appropriate disciplinary actions are taken when staff members have committed privacy breaches;
		5. Report to the Privacy Officer whether disciplinary action was taken;
		6. Notify the individuals affected by an actual privacy breach, as appropriate, after consultation with the Privacy Officer.
	5. **Human Resources (HR)** through its HR Consultants:
		1. Provides required employment information about staff to support investigations;
		2. Support the manager through the investigation process, as required;
		3. Advises on appropriate disciplinary actions to be taken;
		4. Works with managers/supervisors to ensure disciplinary action for privacy breaches is carried out in accordance with HR policies and procedures.
	6. **Medical Directors and Department Heads**:
		1. Inform members of medical staff about complaints or concerns related to suspected or actual breach of privacy;
		2. Advise the Privacy Officer of any alleged breach of privacy and investigations as they occur;
		3. Report any significant breach of privacy involving unprofessional or unethical conduct to the VP Medicine following the process and timelines set out in the Medical Staff Bylaws and Rules.
		4. Notify the individuals affected by an actual privacy breach, as appropriate, after consultation with the Privacy Officer.
	7. **VP Medicine and District Medical Advisory Committee (DMAC)**:
		1. Manage the process for serious privacy breaches that impact privileges, including collaboration with Capital Health’s Board of Directors or the College of Physicians, where appropriate;
		2. Advise General Counsel of any serious privacy breach investigation including the outcome of the investigation.
	8. **eHealth Department:**
		1. Make information and technology resources available to assist in conducting audits and developing and maintaining audit log functionality;
		2. Work with the Privacy Officer to establish standards for audit capabilities in Capital Health electronic information systems containing personal health information;
		3. Identify and maintain a list of electronic information systems containing personal health information and their audit capabilities.
	9. **Procurement**:
		1. Ensure all requests for proposals (RFPs) for electronic information systems containing personal health information have audit requirements that enable compliance with this policy.
2. Capital Health establishes and maintains Privacy Audit Programs as follows:
	1. **Proactive Auditing Program**:
		1. The Capital Health Privacy Officer creates an annual audit plan that defines the types of audits and electronic information systems subject to the Proactive Auditing Program in any given year.
			1. The audit plan defines the type of audits and the frequency with which they will be conducted across the organization, as adapted from time to time based on the results of past investigations, risk management best practices, and feedback from Managers.
			2. The audit plan may vary by system, depending on its audit capability and level of privacy risk associated with the system.
		2. General Counsel approves the audit plan and any significant changes.
		3. The Capital Health Privacy Officer and support staff run proactive audit reports as per the approved audit plan and sends the reports to the user’s manager or Medical Director.
		4. Managers, or Medical Directors in the case of physician users, determine whether the access identified in a proactive report is appropriate or not, based on the user’s defined role and an appropriate investigation into the facts of the case.
			1. Determining whether access is appropriate may involve, but is not limited to the following steps: interviewing the user in question, checking patient records to ensure the user has a legitimate relationship with the patient during the time frame in question, etc.
			2. User access to electronic information systems may be suspended during the course of an investigation into a possible breach of this Policy, on the recommendation of the Privacy Officer in consultation with the Manager/Medical Director.
		5. The Manager/ Medical Director reports back to the Privacy Officer on the results of the investigation, indicating whether the activity listed was authorized access or not and any steps taken to make that determination, within 15 business days of receiving the report.
		6. If the Manager or Medical Director determines that an actual privacy breach(es) has occurred, contact both Human Resources and the Privacy Officer immediately. The Privacy Officer opens an investigation file.
		7. Where an actual privacy breach is found, the Privacy Officer may undertake further audits of the user to determine if there is a history of systematic inappropriate activity and makes recommendations on disciplinary action to the Manager/ Medical Director and Human Resources.
			1. After consulting with each other, either the Manager/ Medical Director or Capital Health Privacy Officer makes the necessary notifications to patients and others.
		8. The Manager/Medical Director ensures appropriate disciplinary action is undertaken as per Capital Health policies, including but not limited to: a warning letter, suspension of access, suspension from work, termination, etc.
		9. The Manager/Medical Director reports back to the Capital Health Privacy Officer on the nature of the disciplinary action taken. The Privacy Officer closes the investigation file.
	2. **Incident-based Auditing Program**:
		1. Any person can report incidents of possible unauthorized or inappropriate access to personal health information stored in electronic information systems involving an individual user(s) directly to the Privacy Officer.
			1. All agents of Capital Health must notify the Privacy Officer if there is reason to suspect unauthorized access to personal health information stored in electronic information systems has occurred.
			2. Staff members can report possible incidents to their Manager and the Privacy Officer using the Patient Safety Reporting System.
		2. The Privacy Officer will conduct a preliminary investigation of the incident and review the audit trails of the systems to which the user had access to see if there is a record of access by the user to the information in question. The Privacy Officer will determine whether further investigation is required after reviewing the applicable audit logs.
		3. If further investigation is required, the Privacy Officer will notify the responsible Manager/Medical Director and steps 2.1.4 -2.19 of this Policy and Procedure are to be followed.
	3. **LET Reporting**:
		1. The Privacy Officer shares the findings of the Proactive and Incident-based Audit Programs with LET in aggregate format annually, or as appropriate. Particularly egregious cases may require the identification of the user involved to LET. Any recommendations for improvements to the program or education will also be submitted at that time.
		2. LET will evaluate the overall effectiveness of the programs based on the findings and any recommendations in the annual report.
3. **Audit Log Requirements**
	1. The Privacy Officer:
		1. Maintains a list of minimum standard fields to be included in the audit logs of electronic information systems containing PHI, as well as suggested additional fields.
		2. Provides the list to the eHealth department and ensures the list is available upon request.
		3. Ensures that, in addition to meeting the needs of the Privacy Audit program, the fields in an audit log are sufficiently detailed for a record of user activity to be generated to give to patients upon request.
	2. Audit logs from electronic information systems containing PHI must be maintained for a minimum of two years from the date of access for audit purposes. (For example, if a user is accessing the system on November 15, 2013, logs must be available at a minimum going back to November 15, 2011).
		1. For exceptions to this rule - based on cost or system performance - request approval from the Privacy Officer.
	3. When working with Capital Health Purchasing to acquire new electronic health information systems containing PHI for which Capital Health will be the custodian, prior to signing a contract, consider whether the audit log of a given system will be able to comply with this Policy.
		1. All other factors being comparable, choose the system with the most enhanced audit log capacity.
	4. If an electronic information system containing PHI does not have an audit log capacity but is a novel technology containing significant clinical care/patient safety benefit, consult General Counsel for approval.
	5. Notify eHealth immediately of all new electronic information systems purchased that contain PHI and their audit capabilities (e.g., the events and fields captured in the audit log, standard reports) as well as anytime the audit capability of an existing system has been modified, in order to maintain a master list of electronic information systems containing PHI. Each system must have a contact person who can generate and explain the contents of the audit log if required and their contact information will be documented by eHealth on the master list.
		1. eHealth updates the master list and provides a copy to the Privacy Officer as needed to develop and modify the organization’s audit plan.
		2. The Privacy Officer will rate the risk of each electronic information system.
4. **Record of User Activity**
	1. All requests for a record of user activity are to be directed to the Privacy Officer. Requestors will be asked to complete a request form detailing the specifics of their request.
	2. The Privacy Officer will review the request, clarify any information with the requestor if needed, and provide the available records within 30 days of receipt of the request form.
		1. The individuals responsible for generating the record of user activity for a given system will provide the record to the Privacy Officer in a timely manner so as to facilitate the meeting of the 30 day timeline. They will also develop a guide for their system that can be provided to patients upon request to explain the content of the record of user activity generated by the system for which they are responsible.
	3. Upon receipt of a record of user activity, requestors are asked to direct questions about the activity in the report to the Privacy Officer, who will follow up with the users named in the report where necessary.

**REFERENCES**

Nova Scotia’s *Personal Health Information Act*

Vancouver Coastal Health’s Auditing Access to Electronic Health Records Policy

AHIMA. “Security Audits of Electronic Health Information (Updated).” Journal of AHIMA 82, no.3 (March 2011): 46-50.

**RELATED DOCUMENTS**

**Policies**

CH 40-045 Corrective Action

CH 50-010 eHealth (Information Technology) Audit

CH 50-015 Computer Password Policy

CH 50-020 Computer End User Acceptable Use

CH 100-100 Privacy

**Other**

Capital Health Privacy Breach Protocol Guidelines

**\*\*\***

**APPENDIX A**

**Minimum legal requirements for the content of a Record of User Activity**

A record of user activity related to an individual’s personal health information must include at least all of the following information:

1. the name of the individual whose personal health information was accessed;
2. a unique identification number for the individual whose personal health information was accessed, including their health card number or a number assigned by the custodian to uniquely identify the individual;
3. the name of the person who accessed the personal health information;
4. any additional identification of the person who accessed the personal health information, including an electronic information system user identification name or number;
5. a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;
6. the date and time the personal health information was accessed or, if specific dates and times cannot be determined, a range of dates when the information could have been accessed by the person. (Personal Health Information Regulations, N.S. Reg. 217/2012, s. 11(2))

**6. Capital Health Written Privacy Statement**

**Your Personal Health Information and its Protection: Capital Health’s Privacy Statement**

As a Capital Health patient, you will be asked to share a variety of personal health information with us so we can give you quality health care and service. Protecting your privacy and maintaining confidentiality is important to us. We understand that personal health information is sensitive in nature. We have information practices to protect your information. For example, all Capital Health employees and associates are required to sign a confidentiality agreement. This brochure will give a general explanation of our privacy information practices.

Nova Scotia’s *Personal Health Information Act* (*PHIA*) and its regulations outline our duty as a custodian to protect the privacy of the personal health information we collect, use and disclose about you. For example, we cannot collect, use or give out more personal health information about you than is needed. Under this Act, you have certain rights and choices around how your information is used and disclosed. This brochure will give you more information about how you can exercise your rights under the Act, such as how to access your health record at Capital Health or file a privacy complaint with us.

**What is personal health information?**

Personal health information is identifying information about you, and includes:

* Demographic information, such as your name, date of birth, address and phone number
* Your provincial health card number
* Your physical and mental health care history
* Financial information related to your payments or eligibility for healthcare

Personal health information can be recorded or unrecorded, such as a printed lab result or a conversation about your wellness plan, and continues to be protected after death.

**Why do you collect, use, and/or disclose my personal health information?**

We collect, use and give out personal information health about you for several purposes, including, but not limited to, in order to:

* Treat and care for you during your stay
* Help other health providers outside of Capital Health who are involved in your care, e.g. your family doctor, community pharmacist, nursing home
* Receive payment for delivering care, e.g. provincial government, private insurer
* Conduct quality improvement and risk management activities, e.g. patient safety reporting
* Conduct patient satisfaction surveys
* Plan and manage our internal operations, e.g. staff scheduling or bed management systems
* Train health professional students support other teaching activities, as we are a teaching hospital
* Conduct approved research, in accordance with *PHIA*
* Notify a representative of your faith group to visit you during your stay, if you identify this group
* Give your family and friends confirmation you are in hospital, your room and telephone extension, and general condition (e.g. fair, good) on the day they request the information
* Enable the Department of Health and Wellness to plan and manage the health care system
* Fulfill other purposes permitted or required by law, e.g. mandatory communicable disease reporting

**How do you collect personal health information about me?**

We collect personal health information directly from you or the person acting on your behalf. Sometimes, we ask other health professionals or health care organizations involved in your care for information to help us provide you care. This may include the health care facility or physician who referred you to us. Occasionally, we may collect personal health information from other sources, if the law allows or with your consent. For example, we may seek information from the Nova Scotia Prescription Monitoring Program to assist us in treating you. Personal health information may be collected and stored in different ways, such as in your paper chart or our electronic information systems.

**When is my consent required for a collection, use or disclosure of my personal health information by Capital Health under *PHIA*?**

Depending on the purpose of the particular collection, use or disclosure, one of the following consent rules will apply:

(a) your consent may be implied from your actions,

(b) your express written or verbal consent is required, or

(c) no consent may be required.

Some examples of each type of situation follow:

 *Knowledgeable implied consent*

In order to provide quality health care to you, we can collect, use and give out your personal health information based on the principle of “knowledgeable implied consent.” This principle requires us to provide you with sufficient information around why we collect, use, and disclose your personal health information and your right to give or withhold consent. This information is provided either through a poster/brochure or a discussion with your clinical team. Once this information is provided, Capital Health can rely on this consent to share your personal health information internally with staff who need to know it to either directly provide or support your care. For example, when you enter an emergency waiting area, you will see posters describing the common uses and disclosures we make of personal health information. If you decide to seek care from us, having had the chance to read the poster, we can assume you are consenting to having your personal health information shared with the appropriate Capital Health staff and associates in order to care for you. This may include

* physicians
* pharmacists
* medical lab technicians
* dieticians
* ward clerks

Unless you tell us otherwise, we may also assume on the basis of knowledgeable implied consent that you agree to us sharing your personal health information with other health professionals outside our organization who are involved in your care. For example, we would share your personal health information with your family doctor or the staff at the nursing home you are live in so they can care for you once you return home.

This standard also applies to our teaching activities. As an academic health organization, we help train large numbers of health professional students each year as they pursue their chosen careers. Real life experience interpreting health information and interacting with patients are key parts of their training.

*Express consent*

Some examples of when we must obtain your express, stated consent include:

* Disclosing your information to the media, fundraising bodies, or marketers;
* Using or disclosing your information as part of research studies. Note: Some research studies do not require your consent and have safeguards in place, such as Research Ethics Board review and approval, to protect your privacy;
* Giving insurance companies, employers or your legal counsel access to your health record;
* Disclosing anything other than general information to your close family and friends, i.e. the fact that you are our patient, your location, and general condition (e.g. fair, good) to your family and close friends, on the day they ask.

*No consent required*

In certain situations we are permitted or required by *PHIA* to collect, use and disclose your personal health information without your consent, including, but not limited to:

* Billing provincial health plans
* Responding to a court order
* Planning and managing our internal operations
* Conducting quality improvement and risk management activities, e.g. patient safety reporting
* Enabling the Department of Health and Wellness to plan and manage the provincial health care system

**Can I decide who can and can’t access my personal health information?**

Under *PHIA*, you have the right to ask that your personal health information not be collected, used or disclosed or to limit its use and disclosure, in cases where your consent is required. For example, you could ask us not to give out your personal health information to a specific health professional or organization. In response to a request, we are required to:

* Take reasonable steps to comply with your request.
* Advise you of any consequences of your request (e.g. the lack of information may result in an adverse event with your care or one of your health professionals may not feel confident that they have sufficient information to care for you).
* If we consider the personal health information to be reasonably necessary to share (e.g. we consider the information clinically important to share in order for you to receive safe follow up care), we must tell the health care professional or organization that we are not releasing all of your personal health information to them because you have not given us your consent to do so.

**How do I make a request and what can Capital Health reasonably do?**

What we can reasonably do varies depending on the nature of your request. Currently, patients who want to keep outside callers from confirming they are a patient can tell staff working in the area upon admission. If you want to prevent a Capital Health staff member or associate from looking at your personal health information on one of our electronic information systems, we can audit some systems to verify they have not done so. Please talk to your care team about any concerns you may have. Or you may contact the Capital Health Privacy Office using the information at the end of this brochure.

**Can I request a copy of my personal health information? How much does it cost?**

You have the right to view or receive a copy of your personal health information. There are a few exceptions. For example, Capital Health has the right to limit your access to your personal health information if your clinical care team here decides that your access could result in a risk of serious harm to yourself or others. *PHIA* sets the fees we can charge for access, which vary depending on a number of things, such as the type of record(s) requested or amount of information you need. We are required to provide you with an estimate of the fees after receiving your completed request, so you can decide whether you want to move forward with the request. We must respond to your request within timelines set by *PHIA*.

Your request to access your personal health information can be made to our Access to Personal Health Information Team. For more information about the process, please call (902) 473-5512, or visit Capital Health’s website for our office locations. The request form can be obtained from the website, in person, or mailed or faxed to you at your request.

**Can I request that something in my personal health information be corrected?**

Yes. You must make your request in writing to the Manager of Health Information Services. To obtain the Manager’s contact information, please call Health Information Services toll free at 1-877-410-0014. Requests for changes to source documentation generated within Capital Health will be reviewed and responded to within 30 days of receipt. There are certain exceptions where we are not required to grant your request, such as when the information consists of the professional opinion or observation by our staff.

**Can I ask to see a list of who has looked at my personal health information?**

Under *PHIA*, you have the right to request a list of users who have looked at your personal health information on our electronic information systems. This list is called a “record of user activity” in the Act. Some systems have the ability to keep this list. You can request a record of user activity from the Capital Health Privacy Office using the contact information at the end of this brochure. We will provide the record to you within 30 days of receiving your request.

**How do you protect my personal health information?**

Capital Health has a number of administrative, physical and technical safeguards to protect your personal health information. For example, we grant role-based access to electronic information systems containing your personal health information. This means that the level of access a staff member is given is tied to how much information is needed to do his or her job. For example, clinical staff have broader access to personal health information than most administrative staff in order to provide care. Also, our policies and staff training reinforce that staff are only authorized to access personal health information they need to know. We can audit some electronic information systems to ensure compliance. Other safeguards include, but are not limited to:

*Administrative Safeguards:* Capital Health has policies that govern how staff and associates manage your personal health information. These include policies that cover:

* privacy
* release of information
* retention of information
* security of information during transport

Staff, physicians, volunteers and students also must make a pledge of confidentiality. This pledge outlines their responsibility to protect your personal health information.

*Physical Safeguards:* We have a number of physical safeguards, such as locked cabinets, secure fax and storage of health records, screen savers for computer terminals and photo identification for staff.

*Technical Safeguards:* Access to electronic personal health information is password protected. All databases must be saved on secure networks and personal health information is located within a firewall for protection.

**What happens if you lose my personal health information or someone who isn’t authorized to see it gains access to it?**

If there is a privacy breach involving your personal health information and we believe this breach may cause you harm or embarrassment, we are required to notify you of the breach. If we don’t notify you, we are required to notify Nova Scotia’s Review Officer for *PHIA*.

**Can I make a complaint if I think you have not followed *PHIA*?**

Yes. Please come to us first if you are not happy about something that has been done with your personal health information. To discuss your concern and see what can be done, in addition to speaking with your care team, please contact our Privacy Office, which can provide you with more information and a complaint form. Under *PHIA*, you must make your complaint to Capital Health in writing.

**What if I am not happy with the way your organization has handled my complaint?**

You may request a review under *PHIA*. The Review Officer for *PHIA* can be reached at:

Review Officer

Personal Health Information Act

P.O. Box 181

Halifax Nova Scotia B3J 2M4

Phone: 1-902-424-4684

Toll-free: 1-866-243-1564

Fax: 1-902-424-8303

**How do I contact the Capital Health Privacy Office?**

For more information about our privacy policies and practices, or to access the services the Office provides as described in this brochure, please contact:

Capital Health Privacy Office:

Rm 1031-D, Centennial Building

1276 South Park Street

Halifax, NS B3H 2Y9

Phone: 902-473-4866

Email: privacy@cdha.nshealth.ca

Fax: 902-473-7850

**7. Capital Health’s Notice of Purposes**

**Capital Health and your Personal Health Information**

At Capital Health, we are committed to protecting the privacy of your personal health information. We collect, use and disclose the personal health information you entrust to us for a number of purposes, which are summarized in this notice. Our employees and other authorized persons are only authorized to collect, use and disclose the personal health information needed to fulfill their roles and for purposes permitted under Nova Scotia law, in particular the *Personal Health information Act (PHIA)*.

**Collection of Personal Health Information**

The personal health information that we collect may include:

* Your name
* Address
* Date of birth
* Health history
* Provincial health card number
* Other information about the tests, procedures and care you received.

We collect personal health information directly from you or the person acting on your behalf. Sometimes, we ask other health professionals or health care organizations involved in your care for your personal health information to help us provide you care. We may collect personal health information from other sources, if the law allows or with your consent. Personal health information may be collected and stored in different ways, such as your paper chart, electronic files and images. We collect personal health information as needed to support the services and activities described below.

**Uses and Disclosures of Personal Health information**

We use and disclose your personal health information in order to:

* Treat and care for you during your stay.
* Help other health professionals outside our organization who are involved in your care to provide health services to you. This could include your family doctor, pharmacist or nursing home staff.
* Receive payment from your provincial health care plan, private insurer, or other body for delivering care to you.
* Support Capital Health’s educational activities, as we are a teaching hospital.
* Conduct quality improvement and risk management activities.
* Conduct patient satisfaction surveys.
* Conduct research, if you give your express consent. Note: Some research studies do not require your consent and have safeguards (e.g., Research Ethics Board approval) to protect your privacy, as per *PHIA.*
* Give your family and friends confirmation that you are in hospital, your room and telephone extension, and general condition (e.g. fair, good) on the day they request the information.
* Notify a representative of your faith group to visit you during your stay, if you identify this group.
* Plan, administer and manage our internal operations, e.g., bed management, staff scheduling.
* Enable the Department of Health and Wellness to plan and manage the health care system.
* Fulfill other purposes permitted or required by law, e.g., reporting abuse.

**Your Rights**

You may withdraw or withhold your consent for the following uses and disclosures of personal health information and we will do what we reasonably can to comply with your wishes:

* Confirmation of your status as a patient. As soon as you are admitted to hospital, please let staff working in your unit or department know that you want this information kept private.
* Use or disclosure to a specific health professional or to a health organization involved in your care.
* Educational Activities
* Patient satisfaction surveys or religious representative notification.

For more information about your rights in relation to your personal health information, please speak to your care team or refer to our privacy pamphlet or privacy website at: http://www.cdha.nshealth.ca/privacy-confidentiality.

1. **June 1st PHIA Readiness Checklist for Managers / Medical Directors**
* Have staff, physicians, learners, etc with AD accounts in your area completed the mandatory LMS privacy course and affirmed the confidentiality pledge as part of the course?
* If you taught the staff with AD accounts via a classroom session, have you sent their names to the Privacy Office so the LMS system can be update?
* Have those without the ability to take the course online been identified? Have they taken part in a classroom type instruction from a staff with access to the LMS course and signed/confirmed the confidentiality agreement from the intranet?
* Has the notice of purposes poster been placed in registration/admission/ waiting/entrance areas? Are the appropriate staff familiar with the notice and able to assist patients with basic questions about the document?
* Have the new privacy awareness/PHIA posters been posted in places likely to come to staff/patient’s attention?
* Have you ordered patient education pamphlet on privacy and made copies available in your area? Are staff familiar with its contents?
* Have you sent out the “FAQs for staff” electronically to your staff for their review?
* Have you held a team meeting to allow for follow up discussion on questions or concerns and further discuss of materials in the toolkit?
* Do your staff know what to do if one of the following happens:
	+ If they identify a possible privacy breach in your area?
	+ If a patient requests a copy of their health record?
	+ If the patient requests that their information not be disclosed to a certain provider or organization?
	+ If the patient requests a correction to their health record?
1. **Privacy Quick Reference Guide**
2. Privacy Breach Reporting/Patient Notification:
* Follow the Privacy Breach guidelines on Capital Health’s Privacy website;
* Submit a report using the Patient Safety Reporting System
1. Disclosure Rules (i.e. who can I share personal health information with):
	* See Capital *Health’s Release of Information from Health Record* policy (CH30-015) If you still have questions after reviewing the policy, contact your manager or the Privacy Office at 473-4866
2. What if a patient wants a copy of their heath record?
* Patients can get the request form off the internet on Capital Health’s privacy website; they can call 473-5512 to ask Capital Health’s Access to Personal Health Information Team for help
1. What if patients want to request a correction to their health record?
* They submit their request in writing to the Manager of Health Information Services
1. What if patient wants to make a privacy complaint?
* They can make their complaint in writing to Capital Health’s Privacy Office.
1. Where can I go if I need for more information about privacy at Capital Health?
	* Staff can refer to the legal services website: http://chdintra.cdha.nshealth.ca/departmentservices/legalServices/index.html
	* Staff can refer the public to Capital health’s public privacy website: http://www.cdha.nshealth.ca/privacy-confidentiality
2. **Core Privacy, Confidentiality and Security of Patient Health Information Policies (as of May 1, 2013)**

The Capital Health policies listed below were identified by our *PHIA* Implementation Committee as being the core policies dealing with the privacy and security of personal health information. They set out rules for a variety of issues, such as release of health information, transferring paper records securely offsite, and destruction of confidential information that apply across Capital Health. The list, while not exhaustive, is intended to act as a quick reference guide for staff with questions about what policies currently exist.

|  |  |
| --- | --- |
| **Core Privacy, Confidentiality and Security of Patient Health Information Policies**  | **Policy Number** |
| Privacy | CH 100-100 |
| Release of Information from the Health Record | CH30-015 |
| Release of information Restriction –Verbal Communications Black out | CH30-014 |
| Security of Health Information during Transport  | CH30-061 |
| Confidential Waste Management | CH90-015 |
| Administration of Research | CDHA RS 01-001 |
| Retention of Records | CH100-055 |
| Retention of Research Records | CDHA RS 01-011 |
| Computer Password | CH 50-015 |
| Computer End User Acceptable Use | CH 50-020 |
| Internet Access/Use | CH 50-005 |
| Acceptable Encryption | CH 50-040 |
| Email Acceptable Use | CH 50-045 |
| Remote Access | CH 50-070 |
| Interacting with Law Enforcement Agencies | CH 100-065 |
| Media Relations | CH 70-025 |
| eHealth Information Technology Audit | CH05-010 |

1. Associates means learners/students, physicians, volunteers, Capital Health Board members, contractors, and other authorized representatives or agents. [↑](#footnote-ref-1)