OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report PH-2013-001

February 11, 2013

Western Regional Health Authority

Summary: The Office of the Information and Privacy Commissioner (OIPC) received two Privacy Complaints under the *Access to Information and Protection of Privacy Act* ("*ATIPPA*") from two separate individuals regarding the Western Regional Health Authority ("Western Health"). Each of the Complainants alleged that their personal health information was not adequately protected pursuant to section 36; was improperly used pursuant to section 38; and was improperly disclosed pursuant to section 39, of the *ATIPPA*. The complaints were broad in scope, expressing concern over the number of people who had access to patients' personal health information, what personal health information could be accessed, and for what reasons that access could occur. Specifically, the complaints were directed at concerns about the electronic records system in use by Western Health, known as Meditech.

Subsequent to receipt of the complaints by the OIPC, the *Personal Health Information Act* ("*PHIA*") was proclaimed into law. The Commissioner found that had this legislation been proclaimed at the time the Complaints were filed, they would have more properly been brought under that *Act*. Furthermore, as Western Health is bound to bring its personal health information policies and practices within the scope of *PHIA*, the discussion and recommendations of this Report are in accordance with *PHIA*. This ensures that the recommendations made in the Report will be forward-looking, useful and relevant to Western Health and to the complainants.

As a result of the investigation conducted by the OIPC, the Commissioner found that the current electronic system being used by Western Health for employee access to personal health information did not meet the requirements and standards of *PHIA*. The Commissioner found that individuals in many roles within Western Health have greater access than is always necessary, even though it is possible to further limit access. Consequently, the Commissioner determined that by permitting such open access controls Western Health was improperly using personal health information and did not have adequate information procedures as required by section 13(2)(b) of *PHIA*. Western Health justified the current framework on the basis that there are practical limitations for controlling access based on each individual user. Nevertheless, Western Health acknowledged that further and better

controls, based on employee roles (i.e. required tasks and duties) could be implemented and it, in fact, Western Health is investigating and implementing these controls. The Commissioner was advised that a move to a newer version of Meditech across the province has been discussed, however its introduction is not yet certain as it has not yet received approval from the Department of Health and Community Services. Once approval is granted the system would take approximately 3-5 years to implement. This new version of Meditech would allow for better access controls and would be based to a greater extent on a role-based access model. The Commissioner found that Western Health has developed and continues to develop policies and procedures with respect to the collection, use, disclosure and security of personal health information which help to mitigate its failure to appropriately limit employee access to personal health information. Additionally, Western Health has an auditing system in place which is designed to track employee access to personal health information and to identify inappropriate instances of access. This system has recently been upgraded to ensure that the most robust form of auditing is employed such that access can be monitored continuously and in real time.

The Commissioner thanked Western Health for their full cooperation in the investigation. Nevertheless, given the current focus on the development of electronic medical records and electronic health records within the healthcare sector there is a need for continued vigilance by regional health authorities to ensure that privacy protection keeps pace. The Commissioner made a number of recommendations to better ensure Western Health's compliance with *PHIA*.

Statutes Cited: *Personal Health Information Act* S.N.L. 2008, c.P-7.01 sections 2(1)(aa); 5 (1)(2)(3) and (5); 4(1)(a); 13 (2); 15 (1); 24(3); 33(2) and (3); and 35.

Authorities Cited: British Columbia OIPC Investigation Report F10-02

Other Resources Cited: The Canadian Organization for the Advancement of Computers in Health ("COACH") 2011 Guidelines for the Protection of Health Information

I BACKGROUND

[1] On July 7, 2009 this Office received two Privacy Complaints against the Western Regional Health Authority ("Western Health"). The Complainants stated that their personal information had not been adequately protected, had been improperly used and had been improperly disclosed contrary to sections 36, 38 and 39 of the *ATIPPA*.

[2] The Complainants described their Complaints as follows:

> **Complaint 1**
>
> *Lack of privacy and confidentiality of patients' medical info and records in the electronic health records system of Western Health. These records are accessible to healthcare workers with whom the patient has no referral or contact on a "might need to know" basis and with no control possible by the patient of detailed health info.*
>
> **Complaint 2**
>
> *Presently our medical records are accessible to 11 groups of health care workers. I did not give permission for my file to be used this way. The more groups that have access, the greater the chance of confidentiality breach.*

[3] Even though they filed two separate Complaints, the Complainants have acted collectively in this matter and, therefore, I have decided to address their Complaints in one Report.

[4] It is also important to note that following the initiation of the Complaints, the *Personal Health Information Act* ("*PHIA*") came into force. Had this legislation been proclaimed at the time the Complaints were filed, they would have more properly been brought under that *Act*. Regardless of what act was in force at the time the Complaints were filed, it must be recognized that Western Health is now required to bring its personal health information practices in line with *PHIA*. Consequently, the discussion and recommendations contained in this Report will be focused on compliance with *PHIA*.

[5] On August 17, 2009 this Office contacted Western Health by letter regarding both Complaints and asked Western Health a lengthy series of questions in an attempt to gain a clear understanding of the controls, protocols, technical limitations and capabilities, and any other related aspects of Meditech, which is the electronic medical records system employed by Western Health. This Office

also requested a submission from the Newfoundland and Labrador Centre for Health Information ("NLCHI"), a Crown Agency that is responsible for the development and implementation of a confidential and secure provincial electronic health record. NLCHI is required to be both *PHIA* and *ATIPPA* compliant. NLCHI designed and implemented the first provincial client registry specifically for the electronic health record, and the first provincial Picture Archiving and Communications System (PACS) that uses a central provincial archive for images and reports, and it has contributed to the national agenda for development of the electronic health record. For these reasons, this Office sought the input of NLCHI in this matter.

[6] On October 16, 2009 a substantial response was received from Western Health. It included a detailed response to a majority of the questions posed, along with supporting documentation (including documents from NLCHI which Western Health supplied on behalf of NLCHI). Western Health also facilitated a site visit from an Analyst investigating this matter to assist in explaining the Meditech system in use, as well as offering an opportunity to clarify any issues addressed in its written submission.

[7] Throughout this investigation the Complainants have also actively provided additional information, resources and documents in support of their Complaints. A meeting was held with the Complainants to allow them to advance any additional arguments and provide additional information to the Analyst investigating this matter.

[8] A meeting was also held between staff of this Office and an employee of NLCHI who has a particular expertise and knowledge of the technical aspects of Meditech. The purpose of this meeting was to glean the clearest picture possible of the capabilities of that system.

[9] Due to the complexities of the Meditech system, a decision was made to distribute our preliminary findings to Western Health and NLCHI before issuing this Report publicly in order to ensure the accuracy of our findings. Public bodies subject to *ATIPPA* and custodians under *PHIA* should not assume that this will become standard practice for all Reports produced by this Office. I do not anticipate taking this step for any access to information reviews, and only for those privacy investigations where I consider it to be of necessary assistance in discharging my duties as Commissioner.

II INFORMATION PROVIDED BY WESTERN HEALTH AND THE NEWFOUNDLAND AND LABRADOR CENTRE FOR HEALTH INFORMATION

[10] In the combined response received by this Office on October 16, 2009 from Western Health and NLCHI, Western Health included a written response to the questions asked and sixteen (16) indices, including: access and privacy policies; the NL DIPACS manual; IT policies; health records policies (both implemented and draft); records management policies; draft information management policies; presentations; forms; memoranda; sample audits; educational and promotional material; correspondence; and electronic health records documents and information (provided by NLCHI).

Western Health

[11] I do not believe it is necessary or practical to quote the entire written response provided by Western Health; however, some points should be highlighted:

> *In 1998, under the direction of the Department of Health and Community Services (DoHCS), Western Health's legacy organizations, the Western Health Care Corporation (WHCC) and Health and Community Services Western (HCSW), entered into a joint purchase agreement for several software modules from Medical Information Technology Inc. (Meditech).*
>
> […]
>
> *The implementation of the Meditech system in the Western region began in 1999.*

[12] The submission from Western Health confirmed that Western Health is currently running version 5.54 of the Meditech "Magic" platform but plans to upgrade to a new version in the near future; however, the update will still not implement the newest version of Meditech. It is the practice of Western Health "not to install the most recent version of any software until it is known to be stable in other installations, unless there is a compelling reason to upgrade."

[13] Western Health provided the following overview of Meditech:

> *Meditech acts as both a portal and a repository for patient information. Each Meditech module provides a user interface which presents information to the user.* […] *The data captured in Meditech is stored in Meditech's native database and backed up on Western Health's data storage infrastructure which is housed in the data centre at Western Memorial Regional Hospital (WRMH) in Corner Brook.*

> […]
>
> *Generally, the Meditech system is used to capture information about a current encounter, with a cumulative history being compiled from the patient's first encounter from 1999 onward. The only exception would be the standard "History and Physical" which is dictated and transcribed upon a patient's admission into hospital. This would include any self-reported medical history from the patient as well as relevant information that the attending physician would glean from the paper chart. There are no limitations enforced by the system in terms of collection and retention other than the limitations of the system interface itself (e.g. there is currently little capacity to capture nursing notes in Meditech).*
>
> *Up to this point in time, Western Health generally has not limited the collection and storage of personal information in Meditech as a result of requests from patients simply because up to now, to our knowledge no patient has come forward with a request. However, we are aware that the option for limited consent is included in the Personal Health Information Act (PHIA) and that we must be prepared to respond to such requests once the PHIA comes into effect.*
>
> […]
>
> *The sources of all information entering the Meditech system are recorded at the record level. This is true whether the source is a user manually keying information or an external system or device automatically feeding data into the system. The original source is not always apparent to the user accessing the record but, if needed, it can easily* [be] *identified by a user of the source module or external system or by the IT department.*
>
> […]
>
> *Patient identification is part of the registration process. Registration staff use multiple identifiers to positively identify the individual. The primary identifier is the MCP number. This, in conjunction with name, date of birth, and address are usually sufficient. The provincial Client Registry contains demographic information obtained from other systems in the province such as the Meditech systems in the other regions, the MCP database, Vital Statistics, and CRMS. Registration staff also have access to the Client Registry to assist them when information is missing or when there may be some challenge in uniquely identifying an individual from the information directly available. Internally, the individual is assigned a facility-specific Medical Record number which serves as an internal identifier.*
>
> *Names are never disassociated from the numeric identifiers in the course of patient care. Disassociating would only occur when the record is being used for a secondary purpose.*
>
> *Generally, clinical information is never removed from Meditech.*

[14] Currently, Western Health employs the following Meditech modules: Payroll, Accounts Payable, General Ledger, Medical Records (for managing paper charts), Admissions/Discharges/Transfers, various Laboratory modules, Radiology, Order Entry, Scheduling, Patient Care Inquiry and Operating Room Management. Western Health explained that the Patient Care Inquiry ("PCI")

module operates differently from the other modules because PCI acts as a viewer for the data contained in the other modules. Consequently, access to this module would provide broad, almost all encompassing, access to the information contained in Meditech.

[15] Western Health has indicated that no formal privacy impact assessment ("PIA") has ever been performed on the Meditech system. The Office of the Privacy Commissioner of Canada describes a PIA as a process that helps determine whether initiatives involving the use of personal information raise privacy risks, measures, describes and quantifies these risks, and proposes solutions to eliminate or mitigate privacy risks to an acceptable level.

[16] In its submission Western Health also explained that access to Meditech is currently granted upon the completion of a user access request. As part of this request the proposed user must identify the type and level of access being sought, as well as provide a signed affirmation of confidentiality and a supervisor's signed approval verifying that the requested access is appropriate to the proposed user's role and the duties.

[17] Western Health explained that the level of access provided to a user account can be limited in two ways: i) by granting/denying access permissions at the time the account is created and ii) based on the physical location of access. That is to say, certain devices (e.g. computers, printers, and medical devices such as lab analyzers and X-ray machines) can only access a limited amount of information based on the location of the device - usually information which is relevant to the patients in the nearest vicinity. This often occurs on hospitals wards, for example. As I will explain later there is an ability to override the second limitation on access.

[18] Once an account has been created and access is provided, Western Health says that the user may then log-in to the system using a unique user ID and password. The user must actively use the system or it will time-out after six minutes of inactivity and require the user to repeat the log-in process. To access patient information, the user may simply search all or part of the patient's name or a numerical identifier associated with the patient (e.g. MCP number).

[19] Western Health acknowledged that, for certain users, the Meditech system provides more access than is available in a paper chart. Western Health also admitted that "some users groups have been

granted access to more data sources than they require" and also that there are more active user accounts in Meditech than there are actual users.

[20] The explanation provided by Western Health is as follows:

> *Currently there are approximately three thousand eight hundred (3,800) active user accounts in our Meditech system. This number exceeds the number of individual users significantly for several reasons:*
>
> - *Approximately one thousand (1000) of these are physicians' accounts that have to be in the Meditech system even if the physician does not work in the Western region, as it is required that they have a user "mnemonic" for the Meditech Medical Records module.*
>
> - *In many instances individual users have multiple accounts in accordance with the multiple roles they fill on a regular basis. For example, it is common for casual clerical staff to work in several different roles on a regular basis. Our practice has been to create multiple role-specific accounts for these employees. We are currently considering what would be required to establish a one-to-one relationship between users and accounts.*
>
> - *There are a significant number of accounts that are active, but that have expired passwords. The IM department is often not notified of staffing changes that would normally require the termination of accounts. This is another area for improvement in our internal security management processes. However, the regular password expiry setting provides a safeguard in these instances.*

[21] To rectify the problem of the excess access granted to a large number of user groups, Western Health indicated that it intends to engage and interact with these groups to determine what access is, in fact, required of each role in those groups. Western Health began this process in May, 2009 but was prevented from continuing with the process due to increased workload and limited resources. It is the understanding of this Office that this process has recommenced since the initiation of this investigation. Western Health explained that it has attempted to mitigate the effects of such broad-sweeping access by ensuring that all employees of Western Health participate in training on privacy and confidentiality.

[22] Furthermore, Western Health explained that it relies on auditing to target and prevent unauthorized access:

> […] *user access to Meditech PCI is subject to both random and targeted audits. Western Health's IM staff perform PCI audits on a weekly basis with a number of individuals selected at random. Any access that appears questionable is investigated and, if no plausible reason for the staff member*

> *accessing the record can be identified, the employee is contacted and a breach investigation ensues.* […]
>
> *Note that Western Health has been exploring ways to improve its current auditing tools. These options include exploring internal opportunities within our own IT Department as well as appropriate vendors.* […]

[23] In later communications with this Office, Western Health confirmed that audits occur:

> […] *on a weekly basis with a random number of individuals audited for that week. Also, there are requests for audits that may come in as well which we do on an individual basis*

[24] Further follow up with Western Health has indicated that it has purchased and installed a new auditing system. This system has been in use since October, 2012. Western Health has indicated that the new software is much more intelligent and capable of searching, identifying and alerting Information Management personnel of questionable access. The triggers and frequencies for auditing has also been enhanced.

[25] In relation to the ability of individual patients to prevent access to their information within the Meditech system, Western Health explained that Meditech does permit "flagging" of information or records but does not permit "masking". Essentially, Western Health has explained, a "confidential" flag can be placed on a record within Meditech which alerts the user that the relevant patient has concerns about maintaining confidentiality of a particular record; however, the flag does not "mask" (i.e. prevent) access to the record.

[26] Western Health has also indicated that there is an ability to block access to a record in Meditech, however it would require labeling the entire file as "confidential" and then creating an access permission for "confidential" files. This would mean that any user without the access permission to view "confidential" files would not even be aware that the records existed and, equally, those with access permission to view "confidential" files would have access to all such files. Western Health states that it has concerns about this mechanism. From a clinical perspective it points out that there is a possibility that a health care provider may not have all the information necessary to treat the patient or to treat the patient in a timely fashion and also they may not be aware that they do not have all the information related to a patient. Additionally, from a practical perspective Western

Health has indicated that it believes it may not be technically possible to flag certain types of records.

[27] Western Health states that:

> *To our knowledge, Meditech does not offer [masking], nor is it planned in any upcoming version. As Meditech is proprietary "off the shelf" software, we wouldn't expect that the company would entertain including such a major enhancement at our request, except, perhaps for a significant fee. Meditech generally responds to the needs of its customer base overall in adding new features to its software.*

[28] On March 24, 2011 an investigator from this Office met with Western Health to assist this Office in its understanding of how Meditech is used in the day-to-day operations of Western Health and to provide further explanations of how the system operates.

[29] At this meeting Western Health further explained the justification for open or global access to the modules of Meditech either directly or through the PCI module. Western Health advised that the user groups which are involved in the clinical or acute care of patients require broad access because on any given day they do not know precisely which patients they will be interacting with or providing healthcare to or the reasons for the interaction. In other words, the flexibility provided by global access is a necessary component of the ability of certain Western Health employees to carry out their duties effectively.

[30] Following this meeting, Western Health provided additional information to this Office. Western Health identified 17 specific user groups - physicians, nurse practitioners, registered nurses, licensed practical nurses, paramedics, ward clerks, physiotherapists, dieticians, occupational therapists, respiratory therapists, medical records staff, speech language therapists, social workers, operating room technicians, audiologists, management and students – with access to the PCI module and/or access to a large number of individual modules. Only 3 other user groups were identified – diagnostic imaging, EKGs, and laboratory technicians – and these groups did not have access to the PCI module. Access to Meditech by these other groups was limited to specific patients.

[31] Furthermore, as mentioned above, Western Health confirmed that they had recommenced their investigations into what access is, in fact, required of each role and user group within Western Health.

NLCHI

[32] Throughout this investigation, a number of meetings, phone calls and other interactions occurred with Western Health as well as NLCHI.

[33] An employee from NLCHI was able to provide a provincial perspective, and advised that upgrades to the Meditech system may occur for all provincial health authorities in the future and these upgrades could link all the health authorities to one single Meditech system – instead of separate systems for each health authority – and provide better role-based access limitations. Further, he indicated that access limitations broader than those which are currently in place are possible in the current system; however, he also stressed that there are practical and functional difficulties in implementing same.

[34] In the course of our investigation, we also learned a number of things about how Meditech functions. For example, modules within Meditech can be limited. Within each module, menus can be built consisting of a series of "routines" and these menus are then assigned to an individual employee. When that employee then logs into his/her user account in Meditech they may only access what is available in their menu. The creation of these menus and the decision of what is to be placed in an employee's menu is dictated by the employee's manager, in consultation with IT, and based on the manager's knowledge and expertise of what is required of that employee's role in the healthcare system and what information they may need to have access to in order to perform their duties properly.

[35] Furthermore, access can be limited by location. For example, computers in certain hospital wards are assigned location identities and these computers will only display the information for the patients on that particular ward. Essentially what occurs is that when the patient visits a Western Health facility and it is determined that they will need to be admitted to a particular ward, the

patient's records are assigned the location identity of that ward's computer. Only once this occurs can the employees on that ward see that patient's Meditech record.

[36] However, it is possible to bypass this limitation if someone logs in with a user name and password that provides broader access (e.g. a physician). The password will bypass the location settings and allow the user access to whatever information would be available to them on any other computer. Essentially, location-based limitations only work where both the user and the location have access limitations.

[37] With the exception of those who are limited by location-based access limitation, there are a large number of user groups who have access to the PCI module, which as explained by Western Health is a viewer for the other modules. There are certain justifications and practicalities associated with this level of access. Given that access is set at the time the user account is created, to adjust those settings to limit access to specific patients or records based on the information the user would need at any given point in time, would require continuous monitoring and adjusting of the settings of that specific user's account. It would require prior knowledge of what patients would be seen by that user and what information would be required to perform the necessary tasks in advance of the patient actually being attended to or receiving health care. Furthermore, it would also require monitoring to ensure that once the user's interaction with the patient had ended that the access ceased.

[38] To do this would require someone with intricate knowledge of each role within the healthcare system **and** the foresight to know which patients and records would be seen by any employee at any time **or** the constant reporting and requesting of access in advance of each patient visit. It would require a team of information technologists operating every hour of every day.

[39] There may, however, be certain circumstances where it would be possible to know exactly what information and what patients are required for an individual employee to perform his or her duties. However, these circumstances may be very limited and will require some further analysis by Western Health, if not using the current Meditech platform, then the next generation of Meditech. This might create scenarios where employees would have to make individual requests for access to specific records or patients for each patient interaction.

[40] In addition to measures which may serve to tighten access, a robust auditing program is another essential component approach to using Meditech within the parameters of *PHIA*. It has been suggested that auditing on a frequent basis with a large number of triggers would capture a large proportion of improper or unauthorized uses. It is my understanding that the health authorities, including Western Health, were all implementing new auditing systems and tools which are designed to continuously monitor access in real time, capturing many more instances of improper use and disclosure than the present systems.

III INFORMATION PROVIDED BY COMPLAINANTS

[41] This Office met with the Complainants on March 24, 2011, at which time they provided further commentary in support of their position. The Complainants highlighted a number of matters including how sensitive they felt personal health information to be as well as the response they received when they requested that access to their electronic medical record be limited. The Complainants alleged that Western Health advised that while this could be done, there may be negative consequences such as a refusal of service or an inability to provide full services.

[42] The Complainants acknowledged that there are circumstances in which full and immediate access to a patient's records may be necessary and they do not want to be seen as trying to prevent such access. Instead the Complainants insist that such access should only occur when necessary. In the meantime, they asserted that masking (i.e. a mechanism by which a patient can limit the people who are entitled to access their electronic medical records and precisely what records can be accessed) or password protection (i.e. a mechanism which would allow patients to place passwords on their electronic medical record and any user requiring access to same would have to first obtain the password from the patient) should be available to patients to control access.

[43] The Complainants also raised concerns with secondary uses, such as research or other uses outside of the direct provision of healthcare, and the de-identification procedure. The Complainants indicated that in instances where research is being conducted, de-identification (i.e. the removal of all information which identifies an individual) should occur and the patient should be notified that their information is being used for such purposes. It was the Complainants' suggestion that if the

open access provided in Meditech continued it could stifle candid conversations with physicians as there would be concern as to who could later access or use the information. The Complainants added that additional privacy training and education was needed for Western Health employees as they had repeatedly been present during inappropriate discussions involving personal health information (e.g. elevator conversations in the presence of members of the public; discussions in public venues, etc.).

[44] The Complainants explained that they were prompted to file their Complaints following an interaction with a Western Health employee. The employee advised one of the Complainants of the employee's ability to see a certain record in the Complainant's electronic record. The employee explained to the Complainants that such access was necessary as the employee, and many other employees, do not know who they will be seeing during the course of a shift and, furthermore, do not know what the patient's medical issues are or could potentially be. The Complainants believe this is done simply for convenience and is unwarranted.

[45] The Complainants argue that there must be some ability on the part of patients to limit or prevent access to personal health information. It was their position that the current system is reactive and not proactive in protecting patient privacy and confidentiality; it is based on a "might need to know" rather than a "need to know" basis and reacts when there is a breach instead of actively attempting to prevent breaches.

IV DISCUSSION

[46] While the technical aspects of this matter are complicated, the issue I must determine in this Report is straightforward: is the Meditech system which is currently employed by Western Health compliant with the provisions of *PHIA*?

[47] As noted above, the Complaints were filed under the *ATIPPA*; however, since that time *PHIA* was proclaimed and the analysis contained in this Report and the accompanying recommendations are made with regard to *PHIA*.

[48] The information contained in Meditech clearly falls within the definition of "personal health information" as set out in section 5 of the *PHIA*:

> *5. (1) In this Act, "personal health information" means identifying information in oral or recorded form about an individual that relates to*
>
> *(a) the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;*
>
> *(b) the provision of health care to the individual, including information respecting the person providing the health care;*
>
> *(c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;*
>
> *(d) registration information;*
>
> *(e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;*
>
> *(f) an individual's entitlement to benefits under or participation in a health care program or service;*
>
> *(g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;*
>
> *(h) a drug as defined in the Pharmacy Act , a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or*
>
> *(i) the identity of a person referred to in section 7.*
>
> *(2) For the purpose of paragraph (1)(b), "information respecting the person providing health care" means, in relation to that person, the following information as applicable:*
>
> *(a) the name, business title, address and telephone number;*
>
> *(b) licence number; and*
>
> *(c) profession, job classification and employment status.*
>
> *(3) In addition to the matters referred to in paragraphs (1)(a) to (i), personal health information includes identifying information about an individual that is contained in a record that contains personal health information within the meaning of that subsection.*
>
> […]

> *(5) For the purpose of this section, "identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or together with other information, to identify an individual.*

[49] Furthermore, it is equally clear that Western Health is a "custodian" in accordance with subsection 4(1)(a) of the *PHIA*:

> *4. (1) In this Act, "custodian" means a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with the performance of the person's powers or duties or the work described in that paragraph:*
>
> *(a) an authority;*
>
> […]

[50] In relation to the protection of personal health information within the custody and control of a custodian, section 13 of the *PHIA* provides that a custodian must have policies and procedures in place to:

> *13 (2)* […]
>
> *(a) protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;*
>
> *(b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;*
>
> *(c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and*
>
> *(d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.*

[51] The multitude of documents provided by Western Health include numerous policies (past and present), draft policies, and proposed policies directed at: protecting the confidentiality of personal health information; protecting the privacy of patients; restricting access to personal health information; the storage, retention and disposal of records; and unauthorized access to or disclosure of personal health information.

[52] Section 15 of the *PHIA* goes on to state:

> *15. (1) A custodian shall take steps that are reasonable in the circumstances to ensure that:*
>
> *(a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;*
>
> *(b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.*
>
> […]

[53] Consequently, reading sections 13 and 15 together, not only must a custodian have policies and procedures in place in respect of the protection, collection, use and disclosure of personal health information, those policies and procedures must be reasonable and must, in fact, achieve the desired purpose. Therefore, what I must now examine is whether the current policies and procedures set by Western Health for the operation and use of Meditech are in compliance with *PHIA* and if so whether those policies and procedures are being effectively implemented.

[54] Generally speaking, in the healthcare context, where healthcare is being provided to an individual, the custodian may use or disclose the personal health information of that individual – on the basis of the individual's implied consent - with those persons within the "circle of care" of that individual. Subsection 24(3) of the *Act* provides clarification to the concept of "circle of care":

> *24.* […]
>
> *(3) For the purpose of subsection (2), the expression "circle of care" means the persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.*

[55] This is the foundation upon which the Meditech system should operate; employees may use or disclose the personal health information of those individuals to whom they are providing health care, but only for the purpose of providing care or participating in the provision of care.

[56] *PHIA* defines "use" in subsection 2(1)(aa) as follows:

> […]
>
> *(aa) "use", in relation to personal health information in the custody or control of a custodian, means to handle or deal with the information or to apply the information for a purpose and includes reproducing the information, but does not include disclosing the information.*

[57] The *Act* imposes safeguards in relation to the use of personal health information:

> *33.* […]
>
> *(2) A custodian shall not use personal health information if other information will serve the purpose of the use.*
>
> *(3)The use of personal health information in its custody or under its control by a custodian shall be limited to the minimum amount of information necessary to achieve the purpose for which it is used.*
>
> […]
>
> *35. A custodian shall limit the use of personal health information in its custody or under its control to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or a purpose authorized under this Act.*

[58] Western Health has acknowledged "some users groups have been granted access to more data sources than they require" by virtue of having access to a large number of modules, or at the very least to the PCI module. On its face, this does not appear to meet the requirements set out in sections 13(2)(b) (i.e. only the information required "to carry out the purpose for which the information was collected or will be used"), section 33(3) (i.e. the "minimum amount of information necessary to achieve the purpose") and 35 (i.e. only "employees and agents who need to know the information to carry out the purpose for which the information was collected or a purpose authorized under this Act").

[59] Both Western Health and NLCHI have explained the justification for the current access framework. Both have agreed that more narrow access limitations are possible; Western Health has actually begun the process of examining, re-evaluating and editing access limitations where it is possible to definitively say what access is required of a role or user group.

[60] From NLCHI, however, we have learned that the global access granted to so many user groups may have to continue, at least until a newer, more advanced system is introduced and implemented. Until such time, limiting access would require continuous monitoring and editing of each individual user account, which would not be feasible administratively without a significant investment, and even then it might create a different set of problems.

[61] Basically, as it has been explained to this Office, in order to eliminate global access, those actually implementing the access controls would have to be told on a daily basis various degrees of information depending on the level of access that is deemed appropriate. So if access was to be granted on a full patient-level (i.e. the user could only access a particular patient's information, but once the user accessed that patient, the user could see all information associated with that patient), then prior to a health care interaction with a patient, the user would have to contact those persons setting the access controls and inform them what patients they would be seeing for a given day and for how long the interaction would continue. Access would then have to be turned on for that user and those particular patients and turned off once the timeframe expired.

[62] To go one step further, access could be controlled on a patient-level and record-level (i.e. the user could only access a particular patient's information, but once the user accessed that information, the user could only see information associated with that patient that is required by the user to treat or assist in treatment.) However, the same level of interactions and discussions regarding what access is needed and when would have to occur.

[63] This would present significant practical challenges including the time and money involved in employing the people necessary to monitor and adjust the access controls. There may also be an impact on the provision of care. For example, care could be delayed if a user required access to additional records or an extended period of access and to do so needed to make additional calls or requests for such access. There could also be an effect on emergency care as the users in this area cannot predict which patients they will interact with at any given time or what information they will require and, consequently, time would have to be spent during intake of the patient to predict and request the necessary access.

[64] Consequently, based on a potential need to see any piece of information associated with any patient at any given time, Western Health has found it practical to allow global access to many user groups, at the very least to the PCI module, but often to many more modules as well.

[65] In Investigation Report F10-02 from the Office of the Information and Privacy Commissioner of British Columbia, the Commissioner was faced with a similar situation as we have here and heard a similar justification for the overly broad access framework which was in place. He stated at paragraph 75 of that Report:

> *[75] Where there are a large number of users of a system, the administrative burden of determining access privileges on an individual user-by-user basis would be burdensome. It would be inefficient, expensive and ultimately insecure to maintain and monitor that level of complexity in access controls. Instead, by assigning users to roles defined by functions, the access privileges of each user are commensurate with the user's role. Each of the roles in this shorter list cannot, however, be so broad that the need to know and least privilege principles are violated.*

[66] The Canadian Organization for the Advancement of Computers in Health ("COACH") has developed a set of guidelines in relation to the protection of personal health information (the "Guidelines"). Three types of controls are outlined in the Guidelines which may assist in protecting this type of information are identified including the preferred method for controlling access which is:

> *Role-based control, which relies upon the professional credentials and job titles of users established during registration to restrict users to just those access privileges that are required to fulfill one or more well-defined roles.*

[67] In paragraphs 76-79 of Investigation Report F10-02, my counterpart in British Columbia goes on to elaborate on the considerations that should go into creating role-based access controls:

> *[76] The role that is assigned to a user must be based on the tasks and services the user provides. In the case of users that are practising a regulated health profession, those tasks and services must also be within the scope of practice of their profession. It is important to note that the job title or professional designation of a user is not necessarily determinative of their role. The role must reflect the actual health services that the user is delivering, or supporting the delivery of, to clients. Roles must also include information technology ("IT") system administration.*
>
> *[77] In accordance with the need-to-know principle, access privileges for each role should be limited by what types of information are needed to perform the functions performed by that role (for example, such types of information as demographic, diagnosis, clinical case notes and financial information).*

> *[78] The role must also be defined in terms of the transactions that users in that role need to be able to perform within the system (e.g. search by name and/or personal health number, view, update, enter, etc.).*
>
> *[79] Applying the least privilege principle, access should be further limited as much as possible so that users are accessing the least amount of that personal information necessary to perform their job functions in their program areas. At a minimum, users should be limited in terms of the types of personal information that they can access. The users' transactions or access privileges must also be restricted to the least privileges that are necessary for their job*

[68] Consequently, while I accept the justification put forward by Western Health about the practicalities of limiting access on an individual user basis, I must agree with the comments of the B.C. Commissioner that other options are available which are less cumbersome. I do, however, also appreciate that in respect of certain user groups a certain level of role-based access has already been implemented in that not all user groups have access to all modules and that Western Health is endeavoring to further define roles and refine its access controls on that basis. Furthermore, as indicated above, if a new Meditech system is installed in the near future, this system will be based on a role-based framework which has the potential to address, to a large extent, the Complainant's concerns.

[69] I will highlight another passage from the Investigation Report of my counterpart in British Columbia, in order to provide guidance to Western Health in relation to the PCI module and the types of limitations which should be considered as access controls are reviewed and adjusted. At paragraph 81 he states:

> *[81] Universal access to the central index and clinical summary violates the need-to-know principle because not all roles need access to all the personal information contained in these modules. The central index includes not only demographic information and personal health number, but also allergies, next of kin, employment, equipment, funding/eligibility, languages, reports, school/education. While all roles require basic identifiers, the additional personal information should be reconfigured into different groupings and made available only to those with a need to know.*

[70] One of the things Western Health is doing to mitigate the challenges and limitations it is experiencing with Meditech is to use a robust auditing system. Western Health's auditing system currently runs audits on a weekly basis with a number of individuals selected at random who are audited for that particular week. Audits are also run upon request, both internal and external, and on the basis of user or patient. Each audit report is then manually reviewed for a variety of triggers

which might suggest that there has been an inappropriate access to a patient's personal health information.

[71] While this system has been reasonably successful in the past in capturing incidents of improper access and disclosure, Western Health has acknowledged that a better, more comprehensive system was necessary and was installed and in use since October, 2012. The new system greatly reduces the need to filter through and find trends in data by making this process more automated. The new system operates in real time and will audit a larger number of staff activities more quickly using enhanced search criteria to do so. The system better organizes existing Meditech data to capture and report trends without the need for manual review. In using this new system I encourage Western Health to review the most recent version of the COACH Guidelines.

V CONCLUSION

[72] While I have found that Western Health, in so far as its use of Meditech is concerned, is not currently in full compliance with *PHIA*, I accept that Western Health has acknowledged this and is striving toward remedying the situation. Western Health has allowed its employees access to more than the minimum amount of personal health information required by employees based on what is necessary for their roles, and I find that Western Health has, therefore, failed to fully comply with its obligations under sections 13, 15, 33 and 35 of *PHIA*. I also conclude that there are practical and functional challenges and limitations which may be hindering full compliance with these provisions. However, Western Health has acknowledged that better controls involving the further refinement of role-based access for employees could be implemented, and Western Health is currently investigating and implementing such controls. Western Health must continue to work towards this goal, and until such time as this is fully implemented, Western Health will not be in full compliance with *PHIA*.

[73] I fully appreciate the history behind this situation. A number of years ago, Western Health chose Meditech as the software platform which would best suit its needs for many years to come. This platform has been added to and built upon over the years, representing a major financial and administrative commitment. The current reality, however, is that *PHIA* places legislative

requirements on the collection, use and disclosure of personal health information which were simply not in place when Meditech was first adopted. My message as Commissioner leading up to and following the proclamation of *PHIA* has always been that custodians must demonstrably strive towards full compliance even when there are practical barriers which might delay that compliance. This is one such case.

[74] Western Health is not the only custodian using Meditech – it is a common software platform in use in all of our Regional Health Authorities. Furthermore, from what I understand, Meditech is also in use in other Canadian jurisdictions. Most Canadian jurisdictions either operate under or are developing personal health information legislation with similar requirements to *PHIA*, so they have either grappled with the same issues I have addressed in this Report, or they will be doing so in the near future. I would encourage Western Health, if they are not already doing so, to work with other health authorities in this province and even elsewhere in Canada to explore options for Western Health to reach full compliance with *PHIA* by researching and comparing solutions to some of the same challenges being implemented elsewhere.

[75] The choice to move towards electronic records has been made long ago, and it is the right choice for many reasons. That being said, while electronic records solve some problems, they create others. For that reason, it is essential that those problems be resolved or mitigated to the greatest extent possible to protect the privacy interests of patients. *PHIA* is the applicable legal framework, which, when fully complied with, will ensure that those interests are protected. Even though role-based access can be perceived by some to be too privacy-intrusive, robust employee training, auditing, and the implementation of serious sanctions for employees who abuse their access, are just a few of the ways that custodians can balance those concerns. Western Health continues to implement and build on these strategies, and I applaud and encourage the work they have done and continue to do in this regard.

[76] Western Health has also grappled with the limitations of Meditech in terms of masking of patient information. Western Health has outlined the limitations of Meditech in providing this particular option to patients, as noted earlier in this Report. While the individuals whose complaints led to this Report may or may not be satisfied with a further refinement of role-based access, a fully functional masking option is also a good solution to ensure that patients such as these individuals

are able to maintain trust in how their personal health information is handled. It is also a requirement under the consent provisions of *PHIA*. Once again, I encourage Western Health to continue to explore potential solutions to this issue with Meditech as well as through communication with other health authorities in this province and elsewhere in Canada.

[77] I wish to thank Western Health for their full cooperation in this investigation. I fully appreciate that making significant changes to complex systems takes time and money, and has many practical challenges associated with it. Despite these challenges, the government of the Province has declared that *PHIA* is the standard which must be met by custodians, and as Commissioner I must make recommendations to ensure compliance, which I have done in the following section of this Report. Some of the changes I am now recommending may have already been achieved by the time Western Health receives this Report, others may be in progress, while still others will require further time, money, and research. That being said, this Office intends to follow up on the progress made by Western Health in 6 months to see what has been accomplished by that time, and to get a better sense of what challenges still lie ahead.

VI RECOMMENDATIONS

[78] I believe a number of the recommendations made in the B.C. Commissioner's Investigation Report F10-02 are well-suited for this matter as well. They include:

a. A role-based access model should be developed and implemented. Roles should be defined as specifically and granularly as practicable;

b. The amount of personal information within the various modules should also be reviewed so that, in accordance with the least privilege principle, each role only has access to the minimum amount of personal information necessary to perform their functions;

c. The role-based access matrix must be fully documented and regularly checked and updated by Western Health's Information Privacy Office and IT system administration;

d. All users should be assigned a role;

e. All individuals should be advised of and have the option to be flagged as confidential in the system and the ability to change the access controls on their records without having to justify their choice and after being fully and consistently informed of this option.;

f. Staff should be required to complete privacy training each year that includes completion of a comprehensive privacy tutorial with specific modules on privacy issues related to electronic information systems. Completion of this training should be tracked and linked to an annual renewal of user privileges; and

g. Staff must sign an oath of confidentiality when commencing their employment. Oaths should also be revisited and amended as necessary when employees change roles. These undertakings should reflect the "need to know" principle as highlighted in the COACH Guidelines.

[79] I also make the following recommendations:

i. Western Health should work with their vendor, experts and their counterparts in other Canadian jurisdictions to attempt to implement masking controls or similar mechanisms to allow patients the ability to personally control access to their personal health information. Masking is becoming a standard element in personal health legislation across the country and, consequently, other jurisdictions may be able to offer Western Health guidance with this recommendation.

j. Western Health should review the most recent version of the COACH Guidelines so as to ensure that it has a full overview and guidance of how to alter and adjust its current system and to prepare for any new electronic record systems to be installed;

k. The process for further defining roles based on the tasks and functions performed and, in turn, the information needed to perform those tasks and functions should be carried out as expeditiously as possible;

l. A PIA of the Meditech system should be completed by Western Health within 6 months of receipt of this Report.

[80] Under the authority of section 74(1) of *PHIA*, I direct Western Health to write to this Office and the Complainant within 15 days of receiving this Report to advise of its decision regarding the recommendations in this Report.

[81] Dated at St. John's, in the Province of Newfoundland and Labrador, this 11th day of February, 2013.

E.P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador