Health Data Access, Use, and Control for Secondary Uses

Table of Contents
Introduction ........................................................................................................................................... 1
Status as a Legal or Business Record ................................................................................................. 3
Contracts and Business Agreements ................................................................................................. 4
Changing Expectations ....................................................................................................................... 4
Potential for Discriminatory Use ....................................................................................................... 5
A Need to Redefine “Ownership” ....................................................................................................... 5
Factors in the Secondary Use of Data ............................................................................................... 8
De-identification ............................................................................................................................... 11
Provincial and Federal Laws and Regulations ..................................................................................... 12
Individual Control ............................................................................................................................ 12
Stewardship of Health Information ................................................................................................... 14
Conclusions ........................................................................................................................................ 15
Stewardship Guidelines for Stakeholders .......................................................................................... 17
Special Thanks to the Author and Reviewers .................................................................................... 18
References .......................................................................................................................................... 19

August 2016
Health Data Access, Use, and Control for Secondary Uses

Introduction
A section of the Hippocratic Oath states, “What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about” (5th Century B.C.E).

Although the Hippocratic Oath is understood in the context of privacy, it is equally appropriate in the context of access, use, and control of information. The corollary to privacy is the use of the information. Traditionally, healthcare professionals operate under the premise that patients own their health information while the media on which it is recorded (paper or other hard media such as film or electronic media) is said to be the physical property of the healthcare entity that collected or recorded the information.

There is a perception that it is permissible to access and use the information for secondary purposes if one owns the physical media. Linking, sharing, and retrieving information has been made easier by computers. The nature of electronic health information—its ability to be transmitted, shared, and leveraged for a myriad of purposes—has resulted in new and greater uses of health data. As a result, the demand for data has increased as well as the value of the data. This has led to what is referred to as ‘function creep,’ which is the use of information collected for one purpose, then used for a secondary purpose, whether it is research, marketing, or health service evaluation.

A greater variety and number of organizations now hold healthcare data and employ it for uses other than direct patient care, the original purpose for which it was created. The increasing secondary use of health data raises the need to define stakeholder rights and responsibilities. It also requires an increasing focus on the importance of data stewardship at the local level. Both are essential steps in creating consumer trust in the exchange of personal health information and in putting consumers at the center of decisions made about their information. The health sector is information-intensive,
and citizens need to have confidence that their sensitive and personal information will be protected properly.

In addition to providers, health data are also collected and held by governments, health plans, technology and service vendors, researchers, employers, and public health agencies. This diverse set of entities, along with the patient or individual, constitutes the body of stakeholders that must be concerned with health data access, use, and control.

In their report entitled, “Better Information for Improved Health: A Vision for Health System Use of Data in Canada, June 2013, the Canadian Institute for Health Information (CIHI) recognizes four categories of health system data use. CIHI and Canada Health Infoway (CHI) refer to the use of health data to strengthen the health care system as “health system use of data” (previously referred to as secondary use). These four categories describe ways in which data from digital sources may be used to provide better programs of care, better allocation of health system resources and better management and prevention of outbreaks.

The first category is in the clinical setting. In this category, secondary health data can improve quality initiatives and the effectiveness of front-line care. Data can be aggregated and reused by clinicians to evaluate their performance against guidelines, and data can provide insights leading to revised care protocols.

The second category of health system use of data relates to managing the health system. Health data can be used to manage and improve the effectiveness and efficiency of our health system by informing program, policy and funding decisions. Access to care can be increased, and wait-times reduced by understanding patient journeys across the continuum of care, ensuring that patients receive the most appropriate services, providing accurate projections of future health care needs for the population and optimizing the allocation of resources across the system.

The third category is for population and public health uses. In these cases health data can be used to understand illness burdens and population's quality of life, along with management and evaluation of public health interventions.

The fourth use category is in health research. Health data can be used to support research informing clinical programs, health system management and population and public health. This would provide more timely public health surveillance of influenza and other viral outbreaks, data from point-of-care systems used to identify unanticipated side effects and negative side effects of new drugs. (Better Information
It is exciting to see where the electronic health record (EHR) will lead us in the near future as there is so much happening in this field. The use of the data found in the EHR is valuable and can provide opportunities that benefit the health and welfare of Canadians.

The field for the most growth and use of the data is in health research. There are many areas that need to be addressed before the information found in EHRs can be used to full advantage, and these will be discussed in further detail below.

**Status as a Legal or Business Record**

A collection of relevant health data about a patient is the basis of the origins of their health record. The health record is considered both a business record and a medicolegal document, meaning in addition to its clinical significance, it also serves as the legal record that can serve as evidence of the care provided.

International Organization for Standardization, (ISO) defines business records as, “information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.”

It is important to recognize that not all health data and information are necessarily a business or legal record. For example, an individual may choose to create and maintain a personal health record on his or her employer’s Web site. This personal health record cannot be considered a business record of the employer even though it is maintained on the employer's Web site, because the information does not meet the ISO criteria of created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Status as a legal or business record implies that a stakeholder has greater rights to access, use, and control the information than a situation in which the information cannot be considered a business record (Records management, 2016).
Contracts and Business Agreements

Contracts and business agreements that specify what information may be accessed and how it is to be used and protected also play a role in how each stakeholder manages health information and data in its possession. These contracts can take many forms, including patient or individual consents, data use agreements, or nondisclosure clauses.

A special agreement related to data and information use is the so-called opt-in or opt-out agreement (also known as a ‘lock box’) where the patient or individual positively affirms or declines to let specific information be used for specific purposes.

Mr. Donald J. Willison has the opinion that it is not clear if the lock-box provision would apply in the research area as the data are de-identified prior to use, and there is usually no attempt to contact the individual. (Welcome to the Canadian Institutes of Health Research - CIHR, 2016)

Changing Expectations

Canadians want and deserve the best care possible. To accomplish this we have a responsibility to be more involved in our health and well-being. For this to be possible, we require the most up to date, comprehensive, and best available information. We want to be able to discuss all available health care options and potential treatments with our physicians, to know what current wait-times are, what the risks are for any procedures being contemplated and we expect our physicians to have that information available or to direct us on where to find it. (Welcome to the Canadian Institutes of Health Research - CIHR, 2016). This same CIHR report states, “Canadians are aware of the value of the availability of personal health information to strengthen our health care system.” Opinion surveys in 2012 show 68%-70% of respondents support the secondary use of information from EHRs to plan, monitor or evaluate the health care system; anticipate and address public health issues; and prevent improper uses of the health care system. They were also comfortable sharing their personal health information across settings and for research. More than 75% of Canadians are comfortable sharing personal health information with health organizations, Provincial Health Departments, and statistical organizations like CIHI and Statistics Canada, as well as health researchers. The sharing support increased from 80% to 88% if individuals were assured their name and address would be removed and were promised anonymity. The only objection was sharing health information with private
and for-profit organizations like pharmaceutical and insurance companies with over 80% of Canadians not feeling comfortable with this.

As the move shifts from paper to electronic health records, more and more Canadians feel that the information found in EHRs can be used to further support applications of health system use of data. They support the use of this data to promote more effective health care systems and for research that helps the general population of Canadians.

**Potential for Discriminatory Use**

Secondary uses of health information to make employment, insurance, or financial decisions may carry the potential for discrimination against individuals. The more downstream the use is from the original purpose for the information, the greater the potential for inappropriate use.

Whether or not it is mandated by law, users of health information should obtain individual consent, limit access and use of the information to relevant purposes, and ensure that the information is not used unfairly or that it negatively affects the individual.

**A Need to Redefine “Ownership”**

Providers legitimately use health information for a number of purposes – primarily for direct patient care. Health system uses of health data include health planning and decision making, reimbursement, credentialing, legal defense, and quality and risk management. Thus, patients have never had exclusive ownership of their health information, where ownership is defined as, “the ability to exercise complete sovereignty over information—to disclose, sell, destroy, alter, or determine who shall have access to it at will.” (Waller, 2006).

Many organizations that hold electronic health information contend that they have the right to access and use it for legitimate business purposes by virtue of the fact that they possess the information. Challenges arise, however, when access and use of personal health information conflicts with an organization's business purposes, many of which may never provide a direct or indirect benefit to the individual. In the context of health care, the primary business purpose for collecting information is therapeutic, that is, in order to provide specific benefits to the individual. It can be challenging to
defend the use of data (aggregate and anonymous) for ‘the public good’ when it does not provide a specific health benefit to the individual (Waller, 2006).

Patricia Kosseim and Megan Brady have written about the increasing pressure by analysts and researchers to access the large volumes of data in the EHR. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes”, 2008). This leads to mounting pressure to provide more flexibility in health information governance (structures, legislation, policies, practices) which would allow optimal use of health information rich EHRs for the benefit of the “common good.”

Because of these complexities, it is necessary to redefine the concept of “ownership” in terms of access, use, and control of health data by any entity that originates, creates, produces, or holds health information, whether that information is identifiable or not. “Who can do what to which data and under which circumstances?” is the question that must be asked in determining the rights and responsibilities of each stakeholder.

Consent

Informed consent is intended to provide effective control for individuals over their personal information but it may also impede research due to decreasing the amount of data available for research or introduce consent bias in the results. As such, the specific informed consent model challenges the significant advantages EHRs may offer in enhancing research capacity to improve the quality of health and health services in Canada. In its report, “Secondary use of Personal Information in Health Research: Case Studies, 2002”, the CIHR state, “Data protection legislation is rapidly emerging across the country with different requirements applying either at the provincial, territorial or federal level, to personal information generally or personal health information, in the private or public sector. Yet, health services and population health research often crosses provincial or even national borders, requiring broader access to personal health data. By their very nature, therefore, these types of studies can potentially invoke multiple laws with varying, and often, inconsistent requirements.”

CIHR states that there is a requirement to “identify and implement strategies for balancing the right of individuals to have their personal information protected and their desire for improved health, more effective health services and a strengthened and sustainable health system.”

The gold standard for research consent is the informed consent method. There are many issues to overcome in this approach for the use of data found in EHRs. The time
and money to be invested every time the researchers obtained informed consent from each and every patient for the research project would make the project cost prohibitive and would make for a very narrow participant cohort.

An alternative to the specific informed consent model is a broad consent method. The consent would be obtained from individuals at the same time EHRs are created and implemented. The individuals know and understand the terms and conditions, and potential research use of EHR data upfront, in a broad general way. This would allow the process to occur without having to re-contact individuals as long as the purported uses respect the general boundaries originally set out. Depending on how it is described, a broad consent may permit specially designated custodians to screen EHR data within the warehouse against specific entry criteria to select potential participants for specific projects. It may allow research data custodians to manipulate EHR data of screened-in participants to efficiently de-identify them and release them to researchers for specific research projects under specific conditions, subject to special arrangements. In special circumstances, where uses go beyond the general boundaries described, individuals would have to be re-contacted to obtain informed consent for research participation. This approach leads to questions about how broad consent would be applied in real world situations. If the consent begins when the EHR is created, what happens with newborn EHRs? Is the data in the EHR not used until the person has reached the age of majority? Would the parents’ consent be acceptable until age of majority? What happens in this case if the patient disagrees with the use of the data? What would happen to the information that is used? How would the person delete the information or the consent?

A key consideration is that not all EHRs are created in an environment that would allow for the time and consideration of all the information a person would need to make an informed decision. An example of this would be if the EHR was created in the Emergency Room of a hospital.

A few other considerations are what level are people allowed to opt out at? Is it at the data element level (i.e. date of birth), highest level (all data) or specific data (lab results)? Does the masking of data include some users, some roles or all users? Then there is the consideration of who can override consent and when this can be done.

Under current law “such an approach [broad consent] would undoubtedly make it easier to do longitudinal health research with large cohorts of participants. It would allow researchers to resolve consent issues with a single consent at the time the individuals are recruited into the [research platform]. There is, however, little or no
legal support for the use of blanket consents in Canada. Such consents are, by definition, far too general to have much legal weight.” Although one could argue true autonomous choice includes the right to waive one's rights to specific information and to make decisions on the basis of whenever and whatever one chooses. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008).

Donald J. Willison, a researcher interested in the use of personal information for health research, has a different approach for an alternative to express and informed consent by using a patient portal into one’s health records. A patient portal is an internet interface where a person can access their personal health information. By using a secure username and password the person can access health information such as recent physician visits, allergy information, and lab results. They may also be able to communicate through emails with their physician, schedule appointments (non-emergency) and update contact information as well as download and complete forms. Use of the portal provides opportunity for individuals to document and communicate their consent choices and allows them to become informed with regards to the uses of their personal information. (Welcome to the Canadian Institutes of Health Research - CIHR" 2016). The use of a patient portal sounds like a promising compromise to the challenges that face the secondary use of patient information in research. It would be interesting to see where this leads in the future of EHRs and the many uses for the information that is contained in them.

Delineating and understanding the rights and responsibilities of each stakeholder are the first steps in developing policies and practices related to secondary uses of health information. These rights and responsibilities can bridge the individual's right to privacy and information technologies capabilities and address such issues as personal control of health information; intellectual property rights when health information is involved; policies related to identity management; and societal requirements that affect the individual's right of control, such as the need for public and population health data. These are a few examples of the very difficult issues that arise in the transition to electronic health information.

**Factors in the Secondary Use of Data**

Currently, there is no single authoritative source, law, or regulation that addresses and defines stakeholder rights and responsibilities. There is a “data stewardship no-man's land” in articulating, and enforcing principles, standards, policies, and practices to
define and reflect the rights and responsibilities of stakeholders. The development of these principles can be guided by several factors that have a bearing in determining what these rights and responsibilities should be with regard to secondary data access, use, and control.

There are many examples of court cases in which the uses of secondary information found in EHRs have had the issue of consent questioned. The law and standards have been very consistent in their handling of the cases. Below are some examples of Canadian cases where it has been upheld that the individual has the right to have control over what information is released and what is done with their personal information.

The case of R. v. Dyment is instructive respective to the question of non-consensual secondary uses of personal health information that was originally collected for medical treatment and used thereafter for a different purpose. In this case, Justice LaForest adopted what was at the time three equally important zones to privacy – territorial, personal, and informational. The individual not only has the right to assert autonomous control over their own property or person, but they have the right to have self-control over their personal information. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008).

Further to this, the Supreme Court of Canada stated in the 1990 decision R. v. Duarte: “privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself.” This includes “all information about a person” not just information that may be deemed sensitive or worthy of protection. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008.) These are examples of how Canadian jurisprudence has clearly and consistently recognized that individuals have legitimate expectations for privacy and the ability to have control over their personal health information and health records. The autonomous control standard is demonstrated through data protection regimes by legal requirement to obtain prior informed consent to the collection, use and disclosure of personal information. Any deviation from this legal standard for health research must be justified and warranted in law according to clear terms and conditions. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008).

In their 2009 publication titled, Data Stewardship: Secondary Use of Health Information, the College of Physicians and Surgeons of Alberta state there is an absence of a formal governance process which provides ongoing review and oversight
of application of “reasonable public expectations” for specific approvals and uses. Monitoring of parallel and unrelated events “impacting overall balance (i.e. “slippery slope” or crossing “tipping point” of incremental impacts of secondary uses) is absent as well. Within the same report they suggest it is necessary to mandate a new governance function to protect the public interest of vulnerable individuals and populations, through setting and monitoring parameters for purposes within “public interest” and “reasonable public expectations.” This process should ensure secondary use rules and principles are applied consistently across the system and respect professional and ethical obligation inherent in primary use. As shared medical records, systemic disclosure of information for primary and secondary uses, and general accessibility of information for secondary uses grows, it is critical that rules application be consistent across professions and organizational boundaries. There should be confidence that when patient information is shared, decisions about secondary use will be made on the same legal basis, and very similar ethical/professional bases.

There are principles for health system use of data which include:

- respect for personal privacy
- openness and transparency of health system uses of data
- oversight and accountability
- patient, health system or social benefit
- balance and reciprocity, and
- the use of non-identifiable information

There appears to be a legitimate concern regarding how personal health data is used and how the government and laws deal with health system use of data found in the EHRs. There is a fundamental protection of the individual's rights that the data used in EHRs for research or other purposes is used appropriately and within the laws.

In his report, Donald J. Willison found that there are a number of challenges in the governance of research use of health information and novel challenges in the context of the interoperable EHR (iEHR). These include:

- the richness of linkable person-level data required for research which makes it almost impossible to de-identify data to the point of anonymity
- indistinct boundaries between research and other uses of secondary information leading to wide disparities in ethical oversight
• growing concern about current ethical standards for consent regarding use of personal health information for health research and the biases into research results and costs of our current two-stage consent process.

There are shifts in the way research is done through data repositories (registries) and bio banks. These platforms of future research challenge existing Fair Information Principles around limits on data collection, use and retention due to no current systemic documentation of the existence of these registries and bio banks. Mr. Willison feels there is a poor fit with conventional consent models within the following areas:

• research and development of research registries and bio-banks
• absence of effective mechanisms to elicit consent choices for range of potential uses of one's personal health information although the advances of the EHR especially inclusion of a patient portal into health records offers a potential solution
• overlapping jurisdictions in oversight of overall research uses of health information could lead to a vacuum in leadership in governance

Willison firmly believes, those managing health information used for health policy analysis and health services research have a responsibility to ensure the confidentiality and security of information, further stating, failure to demonstrate good stewardship of personal information could lead to a loss of public confidence on a scale equal to the tainted blood scandal in Canada and result in the imposition of severe restrictions on our ability to conduct research that will benefit the public. Health Information Management professionals have a role to play as Privacy is one of our four domains of practice.

**De-identification**

De-identified information is that which has been modified so that the identity of the individual cannot be ascertained by a reasonably foreseeable method. Adequate de-identification can be difficult to achieve, and certain levels of de-identification can render data useless. However, the extent to which the data are de-identified can determine which rights and responsibilities apply to information holders.

Full de-identification and aggregation allows the information to be accessed and used to a greater extent because there is less need to control it to protect privacy. Information that has been de-identified with no capability to re-identify, combined with other data can be disclosed, sold, or published without risk of breaching personal right
to privacy. An example might be a January Maclean's article using data from the Canadian Institute for Health Information (CIHI) on the prevalence and incidence of ‘Falls on Ice’ across Canada. Maclean's uses the aggregate data provided by CIHI creating a lead article for a monthly magazine.

According to Kosseim and Brady, in order for de-identification to provide workable and effective protection, there must be clear standards and protocols to minimize risk of re-identification to an acceptable threshold. While de-identification is often heralded as the answer to the consent dilemma, it cannot, alone, provide a universal solution for many forms of health research. De-identification is an elusive and ever changing objective from the standpoint of technology and organization. Standards exist that recognize a wide spectrum of degrees of de-identification, and there is ever-increasing potential for re-identification due to more and more personal information that becomes public. The techniques and practices related to de-identification must always be upgraded to keep up with the increasing risks of re-identification. De-identification in some cases, can provide acceptable means of privacy risk management depending on the purpose and context, but to be truly effective in guarding against risk of re-identification, there also needs to be complementary forms of protection. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008).

**Provincial and Federal Laws and Regulations**

Laws and regulations such as the federal Personal Information Protection and Electronic Documents Act, 2001, the voluntary CAN/CSA–Q830-96 laws, and regulations related to mental health, children’s protection, HIV/AIDS, abuse or neglect, and population health, frequently address rights and responsibilities related to access, use, and control of health information. However, such laws often do not apply to all stakeholders. They may be limited in scope or fail to address secondary uses of health information. The limited extent to which these laws do address policies and practices for stakeholders handling health information can serve as a reference for entities seeking guidance in the development of policies and practices.

**Individual Control**

Although helpful, the preceding factors do not go far enough in addressing the gaps in identifying and understanding stakeholder rights and responsibilities. Control of personal health information must rest with the individual about whom the information
pertains and must be reflected or expressed in public policy and the organizational practices and processes of business and institutional stakeholders.

Deciding on the appropriate level of individual control over personal health information involves balancing important and perhaps conflicting interests such as:

- the right of individuals to access and amend their health information and the complexities of developing a system (whether paper, hybrid or electronic) to facilitate this
- a system that is flexible to meet the needs of all stakeholders (individuals, care providers, facility governance, etc) while avoiding a system that is too complicated
- the desire to increase individual choice, and the desire to reduce complexity and the associated costs imposed on providers, payers, and other stakeholders.

As stated by Dr. Ruth Collins-Nakai, of the Canadian Medical Association, “The primary interests of patients cannot be subjugated by the interests of governments or payers in the name of efficiency or cost savings.” (Canadian Medical Association, 2016).

In the absence of universal regulations and policies, health information management professionals must participate in addressing the critical and ongoing role of stewardship in protecting patient privacy and placing patients at the center of decisions to use their health information (Canadian Medical Association, 2016).

Kosseim and Brady concluded that EHRs in Canada represent more than a simple transformation of paper records to electronic form. EHRs are principally redefining the individual’s right to control the use and dissemination of their personal information in health contexts. The public benefits associated with using EHRs for research purposes continue to challenge the standard of specific, informed consent and its role as the default access control. All in all the legal, ethical and policy difficulties inherent to alternatives to express and informed consent suggest no easy or ready substitute. There is no clear indication that Canadians are willing to cede all meaningful and ongoing control over their personal health information, even in the pursuit of public benefit without there being adequate protections in place and an opportunity to participate in an open and inclusive policy debate over available choices. (Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes, 2008).
Stewardship of Health Information

Stewardship is the process of managing what belongs to another. It requires professional diligence if consumer trust is to be built around data management in healthcare's developing electronic environment.

Even as industry standards emerge and are harmonized, adoption of practices fully respectful of the healthcare consumer and other stakeholders depends, at least in part, on altruistic decision making by originators and holders of data. Stewardship represents a willingness to do what is not explicitly required or readily obvious because it is morally the right, and in some cases, ethical choice. Proper administration of data access, use, and control operations is synonymous with proper administration of privacy protections.

While the industry lacks uniform data access, use, and control requirements, the level of protection afforded an individual's data is significantly dependent on stewardship at the local level. Many questions remain unanswered about how to ensure consistent control wherever data exist, about the appropriate use of secondary data, and how to give the consumer a voice.

After definitions and processes have been standardized, the greatest protections related to access, use, and control of protected health information will be based on administrative handling and responsible human intervention. Any assurances will be vested in organizational philosophy and due diligence manifesting in policies, procedures, practices, and consistent enforcement and follow-through.

Technology introduces new issues and complexities not present in the paper environment because information becomes more pervasive. Some protective practices can be implemented through technology safeguards or with technology assistance. Others can be encouraged with user-friendly technology features. Still more are only as effective as the due diligence and tolerance exercised by data originators and holders within healthcare organizations across the continuum. Despite any technological safeguards, once data has ‘kissed the computer’ the very nature of technology means that the data can be dispersed quickly, in many applications, in many formats making it difficult (if not impossible) to retrieve.

Contractual obligations are usually legally testable. Laws and regulations, though legally testable, may lack compliance monitoring and enforcement. Where best
practices offer guidance, the organization is in full control to create—or not create—what the individual and stakeholders have the right to expect.

When current ambiguity is replaced by an electronic environment of complete standards, heightened regulations, and consistent business practices, stewardship factors affecting data access, use, and control will remain critical. Regardless of the degree of formalized industry control, the need for ongoing respect of stewardship responsibilities will not diminish. Even holders of health information not bound by legal or regulatory compliance directives have an ethical obligation to protect patient health information as any formally bound entity.

Without proper stewardship, we will not establish the trust necessary to implement the electronic health record, health information exchange, and resulting improvements in quality of care, patient safety, and administrative simplification. (See “Stewardship Guidelines for Stakeholders” [below] for 15 actions that lead to responsible handling of patient health information).

**Conclusions**

The gaps in the disparate systems of data access, use, and control contribute to the confusion of ownership issues in health information. Evolving issues such as the pan-Canadian EHR, data repositories, implementation of health information exchanges, and both the use of personal health records (PHRs) and the banking of these PHRs will change this landscape significantly in the near future. Issues related to data access, use, and control will require ongoing monitoring by stakeholders.

Individuals and organizations should approach the application of stewardship by first recognizing that healthcare is patient-centered, and patients must be at the center of the decisions made about their information. This focus requires organizational commitment to continuously review policies, procedures, and practices to reflect the organization’s commitment. This philosophy must also be reflected in consumer education, employee training, and policy and procedure enforcement.

There will continue to be concerns around the control and consent of personal health information. The issues have not changed but will continue to challenge us. The need to come up with alternatives and appropriate ways to provide the information that is in the EHRs for health system use of data will be complex and not easy to resolve. Canadians on the whole support the use of data in EHRs to provide for a better health
system overall, but continue to demand control over who has access and use of their personal information.

Health information management professionals have a valuable role to play in addressing the critical and ongoing role of stewardship in protecting patient privacy and placing patients at the center of decisions to use their health information (Canadian Medical Association, 2016).
Stewardship Guidelines for Stakeholders

- Honor the patient-centric direction of the pan-Canadian EHR agenda; set up policies that keep the patient in control of his or her data wherever possible.
- Initiate data creation, import, and flow processes to ensure appropriate use of quality data by and for the individual, the organization, and the industry to improve quality of care, patient safety, and public health.
- Anticipate broader, external data sharing and health information exchange when establishing an organizational position with data access, use, and control.
- Create a top-down organizational culture that places sound data and information management principles (HIM® and IT) at the foundation of your organization's stewardship philosophy. Set proactive approaches toward optimal protections, rather than leave individuals and the legal system to find holes in your stewardship diligence.
- Adopt a philosophy of reward for staff diligence in protecting health information rather than fear when problems are identified.
- Create a system architecture that maximizes security safeguards and technology benefits that force, help to enforce, and encourage privacy protections and policies. Purchase products aligned with industry-recognized functionality and security criteria.
- Establish internal policies governing your stakeholder responsibilities for optimal data access, use, and control regardless of the absence of external mandates and requirements.
- Aggressively employ accreditation standards and regulatory and legal requirements on the federal, provincial, and local levels. Use standards as baseline expectations regardless of their relevance to your organization.
- Take a non-compromising position toward optimal interpretation of nonspecific regulations and laws. Set up clear, enforceable policies and practices.
- Establish enforcement policies with consistent interpretation and application to staff and business associates in all roles and on all levels. Follow through on punitive steps for proven noncompliance. Make outcomes visible as appropriate and educational.
- Establish or expand the responsibilities of an ethics committee to manage and interpret issues requiring judgment calls and professional accountability and reporting.
- Extend privacy and security principles into all aspects of the data use, access, and control program adopted in the organization. Periodically review and update the program.
- Develop processes to challenge requests for health information that appear to seek more information than is necessary to serve the purpose of the request.
- Establish policies regarding retention and destruction of data when used or created for secondary use. When possible, ensure those policies are enforced after the original purpose is fulfilled and data are no longer needed.
- Educate consumers about their rights and responsibilities regarding the use of their personal health information, including the decisions that will help improve healthcare delivery at the point of care through the availability of information; how to become knowledgeable of and exercise their rights; how to help keep their health information accurate; and tips on detecting fraud.
Special Thanks to the Author and Reviewers

Author:
Tamara Beitel, BA, CHIM

Reviewers:
Sharon Baigent, BA, CHIM
Pat Ramirez, CHIM
Sandra Cotton, BA, CHIM

Editor:
Paula Weisflock, BHA (HIM), MAEd, CHIM

For more information:
To learn more about this and other Professional Practice Resources and the opportunity to earn continuing professional education (CPE) credits based on their content, please contact the Canadian Health Information Management Association.

If you are a subject matter expert in an health information management related area and are interested in sharing your expertise, please contact the Canadian Health Information Management Association to discuss publication of your topic.

Email: chima.education@echima.ca
Tel: 519-438-6700
Toll Free: 1-877-332-4462
Fax: 519-438-7001
Website: www.echima.ca

©2016 by CHIMA. All rights reserved. This report or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of CHIMA.
References


