



**DATA STEWARDSHIP:
SECONDARY USE OF HEALTH INFORMATION**

December 2009

Preface

The topic of data stewardship as pertains to health care is broad, deep and complex. There are many perspectives from which to examine the issues, and many context-specific factors which might apply in determining how to handle health information.

This document is not intended to answer all questions or cover all potential subjects; **nor should this document be interpreted as legal advice.** The comments are intended to assist practitioners in the management of health information – a very dynamic and complex subject. This document has consolidated existing information from a variety of sources as well as the development of new information in response to the evolving needs of Alberta’s physicians. Physicians are encouraged to consult specific resources (such as source College policy papers, the Office of the Information and Privacy Commissioner or the Canadian Medical Protective Association) for detailed guidance on these subjects.

The purpose of this document is to establish and support the College position on data stewardship. The scope of this document relates to the secondary use of information by physicians, adding to the Data Stewardship Framework published in 2006.

This document is intended for use by:

- College staff providing advice or direction to individual physicians
- Individual physicians or groups of physicians engaged in secondary uses of information
- Persons or organizations with an interest in understanding the College position regarding data stewardship and secondary uses of information
- Medical Informatics Committee for ongoing evaluation of data stewardship policies and processes

Executive Summary

Secondary use of health data (using health information for any purpose not directly related to the care of individual patients who are the subject of that information) can enhance health care experiences for individuals, expand knowledge about disease and appropriate treatments, strengthen understanding about the effectiveness and efficiency of our health care system, and support public health goals. In fact, the secondary use of health information is a necessary and accepted part of our health system supporting the effectiveness, efficiency and sustainability of the health system and is an integral part of the cycle of research, medical evidence, and accepted knowledge base through to the delivery of care. Therefore, it is critical to promote and enable secondary uses. It is equally critical to ensure there are adequate safeguards to maintain the balance between public health and patient privacy.

The principles for secondary use are different than those of primary clinical uses. Secondary uses are often directed to populations and impact the broader social, political and cultural aspects of health care more so than clinical medicine at an individual level. The following principles relating to secondary uses are added to the existing College data stewardship principles:

- Respect for personal privacy
- Openness and transparency of all secondary uses
- Oversight and accountability
- Patient, health system or social benefit
- Balance and reciprocity

To meet the principles of openness, transparency, and accountability in an environment where a broad spectrum of secondary uses do not require consent, it is in the interest of the public to have an effective governance model which monitors secondary uses in these contexts. In the current policy environment, there are broadly defined uses in legislation where consent is not required; there are Ethics Review Boards which consider and approve specific uses for research, and custodians who apply ethical judgements in day to day decisions (often with vague definitions and/or categorizations). Absent in this environment is a formal governance process that would provide an ongoing review and oversight of the application of “reasonable public expectations” in specific approvals and uses. The monitoring of parallel and unrelated events impacting the overall balance (i.e. evaluate incremental impacts of secondary uses and reaching the “slippery slope” or crossing a “tipping point”) is also absent.

The mandate of a new governance function would be to protect the public interest as well as vulnerable individuals and populations by setting and monitoring parameters for purposes deemed within the “public interest” and “reasonable public expectations”. The governance process should ensure that secondary use rules and principles are applied consistently across the system and respect the professional and ethical obligations inherent in the primary use, especially where information is shared systematically across professional and organizational boundaries.

Physicians who will be using data or disclosing information, are expected to perform a level of due diligence prior to using or disclosing information for secondary uses. The level of due diligence must be commensurate with potential risks, fulfill legal and ethical duties, and should at a minimum include:

1. Definition of the purpose and data requirements of the secondary use
2. Assessment of the ethical considerations
3. Establishment of the consent model, and engagement of an approval and oversight process as required
4. Establishment of the data and security controls

Table of Contents

1.0	BACKGROUND	1
1.1	Primary & Secondary Uses of Health Information	1
1.2	Growth and Enablement of Secondary Uses	2
1.3	Patient Rights & Expectations	2
1.4	Physician Rights & Expectations	2
2.0	PROTECTING THE PUBLIC INTEREST	3
2.1	The Case for Secondary Uses	3
2.2	A Need for Oversight	3
2.3	A Need for Consistent Rules	4
3.0	SECONDARY USE FRAMEWORK	5
3.1	Secondary Use Principles	5
3.2	General Custodial Duties in the Management of Health Information	6
3.3	Secondary Use Categories	6
4.0	SECONDARY USE GUIDELINES FOR PHYSICIANS	9
4.1	Purpose Definition & Data Requirements	9
4.2	Assess the Ethical Considerations	10
4.3	Establish the Consent Model & Framework	11
4.4	Establish the Data and Control Framework	12
5.0	APPENDICES	13
5.1	Revised Data Stewardship Principles	13
5.2	Informative Examples\Scenarios	17

1.0 BACKGROUND

The primary purpose of the College is to ensure that the public receives safe, quality care from ethical and competent physicians. The College continually monitors trends and issues to identify factors affecting competent medical care as well as changes that enable improvements in medical practice. The past 10 years has seen dramatic changes in medical record processes and the information that is available to and disclosed by physicians. The impact of these changes and the potential to affect both the quality and continuity of care, the relationship between the physician and the patient, and the security and confidentiality of patient information has led the College to focus on appropriate principles for data stewardship.

From the perspective of the College, secondary use of information is both a system-wide issue that requires input and consistent policies from all professions and health delivery organizations; and also a topic where physicians will benefit from having specific guidelines to assist in their ethical and professional decisions.

1.1 Primary & Secondary Uses of Health Information

“A fundamental principle underlying data use is that it is essential to know the purpose for which data was originally collected and that all subsequent processing activities be the same as, or consistent with, the original purpose. This principle, when applied in conjunction with a standardised list of purposes, forms the foundation for a correspondence of permitted purpose between different users, systems, organisations or policy domains who might need to share personal health information.”¹

Primary use – patient health information collected by their physician (or other healthcare provider) for the purpose of providing health services to that patient. Also includes the provider registration information used to document the provision of care. Use of a patient’s health information by another health care provider to provide a service to that patient is still considered primary use.

Secondary use – using a patient’s health information for any purpose not directly related to the care of the individual patient who is the subject of that information. Categories of secondary use (for the College’s data stewardship purposes) include:

Legally required purposes

- Mandated reporting
- At the request of an authorized person

Legally permitted purposes

- Discretionary reporting
- Defined purposes enabled under statute including:
 - conducting research
 - regulatory proceedings
 - providing for health services provider education
 - carrying out any purpose authorized by an enactment of Alberta or Canada
 - for internal management purposes

¹ ISO TC 215/SC N (working draft), Health Informatics – Classification of purposes for processing personal health information

- to assemble a family or genetic history
 - planning and resource allocation
 - health system management
 - public health surveillance
 - health policy development
- Electronic Health Record (EHR) disclosures

Engaging legal advice

1.2 Growth and Enablement of Secondary Uses

We are in an era of dramatic change and enablement for secondary uses due to unprecedented adoption of electronic medical and health records throughout the province and across all sectors of the system. The practical barriers to creating collections of secondary data or the sharing of primary data have been dramatically eliminated due to the electronic format. This format also makes it significantly easier to link data to and from other data sources enabling far more significant profiles and disclosures.

The entire dynamic of primary and secondary data is blurring due to the transition from local Electronic Medical Records (EMRs) to creation of shared EMRs (supporting the care delivery of multiple providers and disciplines) and the use of Electronic Health Records (EHRs). Rather than conscious and explicit disclosures, we now see more prospective disclosures based on defined roles and access privileges. This creates an environment of controlled access versus controlled disclosure. Access is controlled by security authorizations and access methods, while uses and disclosures are controlled by ethics and agreements.

1.3 Patient Rights & Expectations

Privacy and confidentiality of an individual's personal information is a basic and accepted right, well established in common and statute law. Reasonable use of individual information for health system management and to support the need and public interest for ongoing biomedical and clinical research is also generally accepted and is also explicitly defined in Alberta's Health Information Act. Other reasonable expectations include:

- Ethical and professional behaviour and conduct by physicians
- Ethical and legal support for the protection of patient privacy and confidentiality
- A practical consent model for secondary use of patient information
- A patient's ability to access/audit uses and disclosures of their information

1.4 Physician Rights & Expectations

Physicians have a well-established and accepted duty to protect the confidentiality of patients and the data collected during the delivery of care – it is one of the fundamental tenets of the doctor-patient relationship. Physicians are also under a duty to create, use and maintain a patient's health record with a focus on the best interests of the patient. Physicians also have an accepted responsibility to support the health system management goals. Reasonable expectations include:

- Appropriate policy infrastructure that does not interfere with the open and honest information flow between the patient and physician
- Practical implementation of a consent model for secondary uses of information
- Similar standards for consent and for physician privacy in the secondary use and aggregation of their registration information

2.0 PROTECTING THE PUBLIC INTEREST

2.1 The Case for Secondary Uses

“Given the fundamental importance of research and of the importance of human participation in research, we must do all that we can as a society to ensure that research proceeds in an atmosphere of public confidence and trust.” (Interagency Advisory Panel on Research Ethics, December 2008)²

Secondary use of health information can enhance health care experiences for individuals, expand knowledge about disease and appropriate treatments, strengthen understanding about the effectiveness and efficiency of the health care system, and support public health goals. In fact, the secondary use of health information is a necessary and accepted part of our health system supporting the effectiveness, efficiency and sustainability of the health system and is an integral part of the cycle of research, medical evidence, and accepted knowledge base through to the delivery of care. There are also legally required and legally permitted secondary uses which have been established for specific pre-defined purposes to support defined programs and goals. Therefore, it is critical to promote and enable appropriate secondary uses.

However, secondary uses of information can potentially create harm for an individual whose information has been disclosed, and also have material adverse implications and unintended consequences to individuals as well as the health system as a whole.

It is critical to create a policy infrastructure which balances the obligations to improve the public’s health with the need to respect and protect the patient’s autonomy and wishes. In other words, a balance must be achieved between the positive rights of society and right of a patient to privacy and confidentiality. There must also be considerations for the costs and benefits implicit in the balancing of those competing interests. Fundamental to this balancing is the ethical use of information and the professional conduct of all the parties involved, and an effective oversight of the entire process to ensure there is an ongoing balance as appropriate controls and evaluation. The potential value to individual patients and the health system is great, as are the potential risks.

2.2 A Need for Oversight

“... it is in part because such power is vested in public health by law that a code or framework of ethics designed for public health is so very important. The need for a code of ethics for public health, then, might be viewed as a code of restraint, a code to preserve fairly and appropriately the negative rights of citizens to non-interference...

... health professionals must go through the steps of an ethics analysis to assure the public of their integrity. The public must feel confident that public health officials will offer those proposals that will improve the health of the public, that proposed measures are minimally burdensome, and that a fair procedure has determined that the magnitude of the problem and the ensuing benefits justify overriding conflicting moral claims...

... this process, then, must be integrated, constant and ongoing. The most important asset that public health can have is the public’s trust that work is being done on its own behalf. In such a context, public health professionals can and must advocate what they believe, on balance, are the

² Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, Draft 2nd Edition

ethically best approaches for furthering social justice and the public's health.” (Nancy E. Kass, November 2001)³

In an environment where personally identifiable information is shared beyond the control of the physician who collected the information (e.g. EHR networks), to meet the principles of openness, transparency, and accountability in an environment where a broad spectrum of secondary uses do not require consent, it is in the interest of patients who are the subject of that information to have an effective governance model which monitors secondary uses in these contexts. In the current policy environment:

- there are broadly defined uses in legislation where consent is not required;
- there are Ethics Review Boards which consider and approve specific uses for research;
- there are data stewardship committees responsible for the access, use and disclosure of specific data repositories and/or electronic health records;
- custodians who apply ethical judgements in day to day decisions (often with vague definitions and/or categorizations).

Absent in this environment is a governance process that would provide an ongoing review and oversight of the application of “reasonable public expectations” in specific approvals and uses, as well as the monitoring of parallel and unrelated events to evaluate if the sum of individual decisions over time impacts the overall balance between the public's interests and the patient's rights (i.e. evaluate incremental impacts of secondary uses and reaching the “slippery slope” or crossing a “tipping point”).

The College supports the creation of a governance body, spanning health system sectors and groups as well as having public representation, which could provide this oversight. The mandate would be a) to protect the public interest as well as vulnerable individuals and populations by setting and monitoring parameters for purposes deemed within the “public interest” and “reasonable public expectations”, and b) to enable appropriate use of datasets of health information to advance the evaluation of the health system, disease states, healthcare provider and health institution performance, and for patient safety.

2.3 A Need for Consistent Rules

With the growth of shared medical records, the systematic disclosure of information for primary and secondary uses, and the general growth of accessible information for secondary uses it is critical that the application of rules should be consistent across professions and organizational boundaries. Whoever is responsible for information management, be it the solo physician in a community clinic, researchers, Alberta Health & Wellness or Albert Health Services; physicians should have confidence that, when they turn patient information over to these parties, decisions about secondary use will be made on the same legal basis, and very similar ethical/professional bases, that they personally would have used.

³ American Journal of Public Health, Vol. 91, No. 11

3.0 SECONDARY USE FRAMEWORK

The principles for secondary use are different from those of primary clinical uses. Secondary uses are almost always directed to populations and impact the broader social, political and cultural aspects of health care more so than clinical medicine at an individual level. Secondary uses can be the direct use of information for a secondary purpose, but can also be the use of information to identify groups of patients with specific disease states for further intervention at an individual level.

3.1 Secondary Use Principles

3.1.1 Respect for personal privacy

Secondary uses require boundaries and guidelines to offset the inherent loss of personal privacy. In order to respect personal privacy, there must be:

- an explicitly defined secondary use and purpose
- a clear public interest and material value for the defined secondary use
- the least restrictive or coercive methods necessary to achieve the defined purpose
- an ethical framework to balance the public good with the individual loss of privacy
- adequate security and safeguards
- the most limited scope of data necessary to achieve the defined purpose
- the most limited personal identification necessary to achieve the defined purpose
- legal remedies for breaches

3.1.2 Openness and transparency of all secondary uses

Patients have the right to know what secondary uses can occur without their knowledge and/or consent. There should be readily accessible processes (that the physician can either provide or can direct the patients to) which demonstrate among other things the purpose, and the rationale for the use, the information which can be disclosed, and the safeguards that are in place.

Physicians have the right to know what secondary uses of their registration information without their knowledge or consent and have similar processes as patients regarding the rationale and safeguards.

3.1.3 Oversight and accountability

There should be ongoing public policy review and approval of all secondary uses that do not require explicit consent. There must also be periodic review of the cumulative effects of secondary uses on the privacy of individuals. The review must enlist the diverse stakeholders from the health system as well as strong public representation.

3.1.4 Patient, health system or social benefit

Unless required or permitted by law, all approved secondary uses should generally be for the direct benefit of patients, or an indirect benefit to the public through quality improvement of the system. There must be an appropriate balance of the potential benefit, the burden to enable the secondary use, and the expectation that the objectives can be reasonably achieved. Benefits could include:

- effectiveness and/or efficiency of the profession and the health system
- enhance the delivery of care
- enhancement of public safety
- enhancement of professional competence, knowledge, and risk management

3.1.5 Balance and reciprocity

There must be a practical policy in place to enable legitimate secondary uses without placing an undue burden on physicians disclosing patient information.

3.1.6 Use non-identifiable information

To the extent possible, patient and physician information must in a non-identifiable form for any purposes other than the provision of health care services to a patient.

3.2 General Custodial Duties in the Management of Health Information

General duties that a custodian of health information must consider:

- collect, use or disclose health information with highest degree of anonymity possible
- collect, use or disclose health information in a limited manner
- protect health information
- ensure the accuracy of health information

3.3 Secondary Use Categories

The following is a summary, and therefore not a complete list of situations where a physician is under a duty or has the authority to report without the consent of the patient who is the subject of the record.

3.3.1 Legally Required Purpose

Legally required purposes are defined in various statutes and legislation, and the physician is obligated to disclose or use information they have collected for the secondary purpose. These purposes can be mandatory reporting which would be initiated by a physician, or they can be at the request of an authorized person.

Please note: a) the following list is illustrative only; it is not intended to be comprehensive. b) in virtually every legally required purpose listed below, there are exceptions, conditions and situational factors which may apply. Consultation with the CPSA, CMPA or legal counsel is advisable for specific situations.

Mandated Reporting

A physician must initiate the report of:

- Specified communicable diseases, rabies or cancers
- Suspicion of nuisance or threat that may be injurious or dangerous to the public health
- Suspected child abuse
- Suspected abuse of “a person in care”
- Deaths under certain circumstances
- Gunshot wounds and stabbings
- Results of blood alcohol testing, when blood has been drawn at the request of a Peace Officer, who has a search warrant for that purpose
- Medical conditions of flight crews, air traffic controllers and others, where the physician believes that the medical condition is likely to constitute a hazard to aviation safety
- Medical conditions that could be a threat to safe railway operations, for railway workers occupying a safety critical position

- Medical conditions of physician where the treating physician believes that there is a condition that is likely to constitute a hazard to that physician's patients
- Notice of birth; medical certificate of death

At the Request of a Authorized Person

A physician must provide medical information upon the request of:

- The patient, who is the subject of the information (where the patient was the source of that information)
- Court Order
- Any third party (including physicians not involved in the patient's care) only when accompanied by authorization to release
- A patient's legal guardian, with documentation
- A patient's parent, when patient is less than the age of consent (subject to the rights of a "mature minor")
- A patient's parent, when separated/divorced parent has legal custody (and patient is less than the age of consent and subject to the rights of a "mature minor"))
- The executor of the estate, for a deceased patient
- The College of Physicians and Surgeons of Alberta pursuant to
 - an investigation under the Health Professions Act
 - an office visit pursuant to a peer review, PAR Review or other regulatory process
 - an inquiry pursuant to the Triplicate Prescription Program
- Order of a Statutory Board
- The Workers Compensation Board, regarding an injured worker;
- The Therapeutic Products Directorate, Health Canada regarding narcotic drugs
- An agent of the Federal Minister of Health, who is undertaking an investigation under Section 55 of the Controlled Drugs and Substances Regulations (information relating to narcotic prescriptions only)
- A Director under the Child, Youth and Family Enhancement Act who has exclusive custody of a child, may authorize the provision of essential medical, surgical, dental or other remedial treatment for the child that is recommended by a physician or dentist, when the guardian of the child is unable or unavailable to consent

3.3.2 Legally Permitted Purpose

Legally permitted purposes are defined in various statutes and legislation, and the physician can apply discretion and judgement on whether to use or disclose information in specific situations/conditions. These purposes can be discretionary reporting which would be initiated by a physician, specific purposes identified in the Health Information Act as enabled secondary uses or Electronic Health Record disclosures.

Discretionary Reporting

A physician may report:

- Persons medically unfit to drive
- Patients who, the physician has reason to believe, present a clear and present danger to society
- Patients who have been treated for a mental illness ... that was associated with violence or threatened or attempted violence on the part of the patient against any person

- Under circumstances outlined in the *Mental Health Act*, a physician may disclose health information relating to a person receiving diagnostic and treatment services in a centre designated under that Act
- Information can also be disclosed where the physician reasonably believes:
 - that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and that the disclosure will protect the health and safety of Albertans
 - that the disclosure will detect or prevent fraud or limit abuse in the use of health services

A physician need not report:

- Admitted use of illegal drugs
- Injuries suffered during the commission of a crime (except legally required reporting for gunshot and stab wounds)

Defined Purposes Enabled by the Health Information Act

Under the *Health Information Act*, identifiable information can be disclosed or used (subject to consent provisions and other limitations) for the following purposes:

- providing health services
- determining or verifying the eligibility of an individual to receive a health service
- conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline
- conducting research (subject to conditions)
- providing for health services provider education
- carrying out any purpose authorized by an enactment of Alberta or Canada
- for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management
- to assemble a family or genetic history where the information is used in the context of providing a health service to the family member

Defined custodians can also use individually identifying health information in its custody or under its control to carry out the following functions within the geographic area in which the custodian has jurisdiction to promote the objectives for which the custodian is responsible:

- planning and resource allocation
- health system management
- public health surveillance
- health policy development

Electronic Health Record Disclosure

- Under the *Health Information Act*, identifiable information can be disclosed to or used by an information manager (of an Electronic Health Record) for the purposes authorized in an Information Sharing Agreement

3.3.3 Engaging Legal Advice

Physicians can use patient information for the purpose of obtaining medico-legal advice, legal assistance or risk management advice from legal counsel or the Canadian Medical Protective Association.

4.0 SECONDARY USE GUIDELINES FOR PHYSICIANS

Physicians who contemplate using data for secondary purposes, or disclosing information to other custodians or information managers where subsequent secondary uses may occur are expected to perform a level of due diligence. This is both a legal duty and a professional obligation. The level of due diligence and competence must be commensurate with potential risks, fulfill legal and ethical duties, and should at a minimum include:

1. Definition of the purpose and data requirements of the secondary use
2. Assessment of the ethical considerations
3. Establishment of the consent model, and engagement of an approval and oversight process as required
4. Establishment of the data and security controls

4.1 Purpose Definition & Data Requirements

Ensure that there is a clearly defined and articulated purpose for the secondary use.

Determine which category the purpose belongs to and the legal requirements of the category- if you are uncertain which category a secondary use would fit into, contact the College or the Office of the Information and Privacy Commissioner for further clarification.

Legally Required Purpose

- Is a mandatory use
- Does not require patient consent
- Generally has pre-defined reporting format and content, but if not apply the principles and general duties to define the disclosure

Legally Permitted Purpose

- Does not require patient consent
- Requires either a request by a an authorized person or organization or a documented rationale for discretionary disclosures
- May have pre-defined reporting requirements, but still need to apply the principles and general duties to define the disclosure

Engaging Legal Advice

- Does not require patient consent
- Apply the principles and general duties to define the disclosure

Defined Purposes Enabled by the Health Information Act

- Does not require patient consent
- Apply the principles and general duties to define the disclosure
- Identifiable information used or disclosed for research purposes must have an ethics board review and approval (research, as defined by the *HIA* means “academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both”). The approved secondary use:
 - is subject to the conditions imposed by the ethics review board
 - must apply the consent model as directed
 - must collect explicit consent for the collection of any additional information

EHR Disclosures and Uses Enabled by the Health Information Act

- Does not require patient consent
- Requires the ability to ensure the trust of the doctor patient relationship regarding express wishes of the patient regarding disclosures
- Requires an evaluation of the endorsement and recommendations made by the College regarding the specific use or disclosure
- Requires an evaluation of the patient information within the clinical practice in relation to the approved disclosures and subsequent uses as described in the Information Sharing Agreement (which establishes the rules and conditions for subsequent uses of the disclosed information)
- Requires a binding Information Sharing Agreement which articulates the expectations of the disclosing physician as well as the defined uses of the data once disclosed

Establish the data requirements:

- Assess the need for identifiable information
- Determine the minimum data requirements for the defined purpose
- Recognize the inherent limitations of using data for any secondary use where the context is different from the original collection

4.2 Assess the Ethical Considerations

Even if the use is legally permitted or enabled, there may still be ethical considerations to review which may support limited or non-disclosure of information. Review the purpose based on general ethical principles as well as the specific principles for secondary use, and then consider the extent and risk of that use/disclosure. There should be a proportionate level of review – as risk to patients increase, so should the scrutiny, skills and expertise of the physician increase. Specific criteria should include at minimum:

- Evaluate the potential disclosures (intentional and unintentional) as well as the risks to the patients
- Evaluate the potential disclosures as well as the risks to the physician who is disclosing the information
- Ensure there is appropriate respect for personal privacy
- Ensure there are defined potential benefits to patients, health system, or society
- Ensure that potential risks are identified and mitigated, and that there is a reasonable balance of the risks and benefits
- Ensure the need for identifiable information is justified
- Ensure there is legitimate authority for the defined secondary use, and that the use of information is appropriate
- Understand the risks to patients, and their rights, where there is dissemination of identifiable information or a risk of re-identification
- Understand the limits to the completeness, reliability and validity of the data source

If there are ethical considerations identified where there is reasonable doubt that the use would fit within “reasonable public expectations”, or where there is material risk to individuals or groups, the secondary use should be submitted to an Ethics Review Board for review (or in situations where an REB would not apply, such as a Quality Assurance, consider a formalized peer review process).

4.3 Establish the Consent Model & Framework

Non-identifying information can be used or disclosed without consent for any purpose (subject to some conditions).

There are a variety of consent models which can be utilized for secondary uses⁴:

- **Legislated consent** – in place today with specific uses defined in the *Health Information Act* that do not require consent
- **Implied consent for secondary uses with “reasonable public expectations”** – in place today where an Ethics Review Board can enable a secondary use with implied consent. The consent model must be implemented as directed by the ethic review board
- **Implied consent for secondary use for the treatment of another individual or family member** (i.e. treating a newborn and using the birth mother’s information, treating patients with hereditary diseases and accessing parental information) – physician review of the ethical considerations and circumstances of the specific situation and the known wishes of the individuals involved
- **Explicit patient consent for each specific secondary use** – default consent model

Generally, a patient’s right to privacy establishes consent as a requirement for any secondary use or disclosure of their information. In Alberta, the *Health Information Act* considers and specifically enables a wide range of secondary uses and disclosures to be in the public good and therefore to not require consent. The onus is on the user/discloser of the information to justify an exception to either the autonomy principles or the legislated consent provisions.

When the collection of consent is required from a legal requirement or the direction of an Ethics Review Board or other formal ethical review, the patient must be capable of giving consent, be informed of the scope and impact of the consent, and give the consent voluntarily without undue influence or coercion from others.

“Respect for autonomy implies that participation in research should usually be voluntary – a matter of choice...

... Autonomy is not always the paramount consideration. Indeed, for some types of research, free and informed consent is not even required. The real inquiry, therefore, is the extent to which the exercise of autonomy is possible, and whether it can be validly exercised: either directly, by the prospective participant, or by the authorized third-party decision-maker...

... This does not imply that group consent is a condition of ethic approval. The ethical recruitment of participants in human research goes beyond an evaluation of autonomy, which often seems to focus primarily on whether an adult person has signed a consent form. It is a more complex consideration of whether the recruitment of participants has been carried out on a basis that is ethically legitimate and methodically justified. It should be a process that respects and reflects, wherever possible, the values and preferences of the individual participants and, where necessary, engages the groups that may be impacted by the research.” (Interagency Advisory Panel on Research Ethics, December 2008)⁵

⁴ Some accepted consent models are not included as they are not enabled in Alberta’s legal framework – this would include negative consent or broad, prospective implied consent for undefined purposes.

⁵ Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, Draft 2nd Edition

If collecting consent is a requirement, consider the implications of common issues regarding the practical collection of consent:

- the sheer volume of the population and the overhead and the cost of managing the consent (and the detailed data and information supporting the consent)
- cost implications (e.g. diverting priorities or capacity within the system, potentially limiting valid or necessary research, ...)
- retrospective use of information, versus prospective use
- possible introduction of a bias in the resultant information through the consent process
- linking information to consent is in itself a secondary use and a confidentiality issue
- possible introduction of harm by collecting consent (e.g. by initiating unwanted contact, ...)
- the secondary user, or even the primary user may not have an ongoing patient relationship to obtain consent

4.4 Establish the Data and Control Framework

Evaluate the source and quality of the data to be used and determine if there any qualifications on the quality of the data, restrictions that need to be propagated to the secondary data or any other issues related to the primary data.

Review the process for managing data to:

- Ensure there is adequate security in the transfer and storage of data
- Ensure there is a plan to manage the retention and destruction of data
- Ensure there is a process to log the uses and disclosures of secondary data
- Ensure there is a trust model to fulfil the professional obligations of the doctor-patient relationship

5.0 APPENDICES

5.1 Revised Data Stewardship Principles

Inherent in the discussion of data stewardship is a natural tension between conflicting objectives and principles. Given the wide spectrum of practice situations these Data Stewardship Principles offer general guidance. It is recognized that no principles are absolute and can often be in conflict with each other in specific situations. Examples of these types of tension include:

- Information needs of the health system (e.g. research, public health, patient populations, etc.) versus the wants and desires of the individual patient and/or physician
- Patient wishes versus physician obligations/duties
- Public safety versus the privacy of the patient as well as physicians and other providers
- Legal, ethical and best practices versus practical demands of time
- Physician autonomy versus integrated health system care models
- Advanced medical record solutions and data stewardship practices versus manual processes
- Technology advancements versus historical standards of practice.

Autonomy

- Patient autonomy
Patients have the right to self-determination, including in regards to their health care and to the extent possible, to control the management of their information.
- Respect for personal privacy
Secondary uses require boundaries and guidelines to offset the inherent loss of personal privacy. In order to respect personal privacy, there must be:
 - an explicitly defined secondary use and purpose
 - a clear public interest and material value for the defined secondary use
 - the least restrictive or coercive methods necessary to achieve the defined purpose
 - an ethical framework to balance the public good with the individual loss of privacy
 - adequate security and safeguards
 - the most limited scope of data necessary to achieve the defined purpose
 - the most limited personal identification necessary to achieve the defined purpose
 - legal remedies for breaches
- Physician autonomy
Physicians have the ethical and professional responsibility to direct the care of their patients, which includes their information management protocols. Physicians have the right to control the management of information regarding their provision of care.
- Health system management
Physicians have a responsibility to support the planning, management and quality improvement in the health system in which they practice, recognizing the scope of their professional practice and the increasing nature of the multi-disciplinary and cross-organizational nature of the system.

Fiduciary Duties of the Physician

- **Doctor-Patient relationship**
Physicians have a duty to act in good faith vis-à-vis their patients and to protect the confidentiality of the information in their trust. This includes informational privacy (information about the patient) as well as associative privacy (the potential impacts on the patient of the use of the information). This duty requires that physicians limit disclosures (or allowable uses) of identifiable patient information to those with a need to know. And unless the physician is authorized or required by law to disclose the information without consent, requires the informed consent of the patient if the use or disclosure of the identifiable patient's information extends beyond the clinical use for which it was obtained.
- **Beneficence**
A physician has a duty to advance the good of patients in their care, which includes the management of the personal information they hold in trust.
- **Non-maleficance**
A physician has a duty to do no harm to the patient, including through the handling of the patient's information.
- **Maintain a medical record**
A physician has a legal and professional duty to maintain a medical record including the creation, retention and destruction of those records. The physician must retain access to those records consistent with medical record retention requirements and be able to satisfy medical-legal standards for confidentiality, access, document integrity and records management processes.
- **Care delivery**
A physician has a duty to utilize sound data stewardship principles to optimize the quality and continuity of care of patients.

Balance

- **Legitimate infringement**
There is a balance between the individual's control and the needs of society including legal, regulatory and ethical obligations to disclose information.
- **Openness and transparency of all secondary uses**
Patients have the right to know what secondary uses can occur without their knowledge and/or consent. There should be readily accessible processes (that the physician can either provide or can direct the patients to) which demonstrate among other things the purpose, and the rationale for the use, the information which can be disclosed, and the safeguards that are in place.

Physicians have the right to know what secondary uses of their registration information without their knowledge or consent and have similar processes regarding the rationale and safeguards.
- **Pragmatism**
There is a balance between the time required to access/research all information sources and the benefits and risks associated with improved access.
- **Balance and reciprocity**

There must be a practical policy in place to enable legitimate secondary uses without placing an undue burden on physicians disclosing patient information without proper regard for the potential impact to the patient.

Duty of a Custodian / Information Manager

- Custodian-Information Manager Relationship

Custodial responsibility extends to the physical and/or virtual data stored in shared medical records under the contracted control of an Information Manager, such as an EHR or a Shared EMR. The Information Manager must act in good faith and trust to maintain the security and confidentiality on behalf of the custodian who collected the information.

All information sharing relationships should be formalized either as or within a contract, a memorandum of agreement or as an Information Sharing Agreement. The agreement must enable physicians to comply with all medical record obligations, quality assurance processes, and to ensure ongoing access for professional or patient needs. The agreement should address indemnifications, limitation of liabilities and appropriate representations and warranties.

- Information integrity

A physician, as well as the information manager has a duty to ensure patient information is accurate and complete. The collection of information including the procedures, rules and edits applied to the medical record should be considered to ensure that the stored data is made in the context of both the local medical record requirements supporting the delivery of care as well as any known prospective uses (i.e. EHR posting). Considerations should include:

- Accuracy
- Consistency
- Granularity/detail of the data
- Precision
- Comprehensiveness
- Relevance
- Currency/timeliness

Subsequent changes to collected information must be duly noted and propagated to EHRs to preserve an audit trail of changes to documentation.

- Information privacy

A patient is the owner of information pertaining to them maintained in all types of medical records, and has the rights pertaining to:

- confidentiality
- controlled access (enabled by express wishes for masking, limiting disclosures, uses, etc.)
- accuracy of the information, including the right to request corrections
- access to, and obtaining copies of their own information
- access to a record of all accesses to, or disclosures of their information
- basic and controlling interest in the record.

- Defined Uses

Physicians may use and disclose information (with appropriate consent where required) for defined, legal and ethical purposes:

- Information relevant to the care and treatment of patients in a process of providing health care services
- Facilitating good patient management practices
- Data analysis for the betterment of patient populations
- Quality assurance programs
- Research (with appropriate consent and ethics approvals)

Managing Change

- Governance
An effective governance process must be in place to ensure ongoing adherence to data stewardship principles and effective change management. The process must be inclusive of key stakeholders (i.e. professions, Ministry, service delivery organizations, Office of the Privacy Commissioner, the public) and have effective dispute resolution mechanisms and sanctions.
- Continuous Improvement
Physicians have an obligation to evaluate and where possible to enhance the stewardship of patient information where there is opportunity to enhance the quality or continuity of care.
- Oversight and accountability
There should be ongoing public policy review and approval of all secondary uses without explicit consent. There must also be periodic review of the cumulative effects of secondary uses on the privacy of individuals. The review must enlist the diverse stakeholders from the health system as well as strong public representation.
- Patient and/or health system benefit
Unless required or permitted by law, all approved secondary uses should generally be for the direct benefit of patients, or an indirect benefit to the public through quality improvement of the system. There must be an appropriate balance of the potential benefit, the burden to enable the secondary use, and the expectation that the objectives can be reasonably achieved. Benefits could include:
 - effectiveness and/or efficiency of the profession and the health system
 - enhance the delivery of care
 - enhancement of public safety
 - enhancement of professional competence, knowledge, risk management

5.2 Informative Examples\Scenarios

5.2.1 Using Clinical or Billing Data for Quality Assurance/Quality Improvement Purposes

Contemplated Secondary Use – a recently published clinical guideline reported standards for the management of “chronic disease ...” where “defined outcome” could be expected in “x%” of cases. You are considering developing a report extracting data from your electronic medical record to evaluate how your clinical practice compares with the standard.

1. Purpose & Categorized Use

The purpose is quality assurance/quality improvement. You will be using data collected for the care and treatment of individual patients to assess your overall practice. You determine that you need identifiable information as you may need to review individual charts as part of the review process, and potentially schedule patients for follow-up. You have identified that you require five pieces of data from your electronic medical record, and that is the minimal data necessary to perform the evaluation. There will be no disclosure resulting from the secondary use.

The *Health Information Act* explicitly enables the purpose for internal management, which includes quality improvement of this nature as an approved secondary use.

2. Assessment of the ethical considerations

There is limited risk for disclosure. The reports will be used internally within the practice, and the reports will not display identifiable information (other than the chart #) limiting unintentional disclosures. There is no risk to the physician as the report is to be used for his/her own professional use. The data source is a known quantity, as the electronic medical record has discrete fields for the data in question and charting etiquette for the practice to use those fields has been in place since 2006. Reporting will be limited to 2007 and later.

3. Consent model & oversight

The *Health Information Act* explicitly identifies that consent is not required. No oversight is required.

4. Data and security controls

The execution of the report will be limited to authorized users. Storage of the report will require physical controls to ensure there is no accidental disclosure. This is a one-time evaluation - once the review has been completed and follow-up action scheduled, the report will be destroyed.

Assessment – this is a legitimate secondary use with appropriate due diligence.

Variation #1

- You will be evaluating not only your patients, but including all the patients for all the physicians practicing in the clinic.
 - There is a disclosure in this situation, but consistent with the Information Sharing Agreement in place at the clinic which defines the data stewardship principles. You have reviewed the use with your peers and have agreed to collectively review the results.

- One physician identifies a charting technique for his patients where specific instances (noted in the chart) would invalidate the reported values. The patients for that physician would be excluded from the report.

Variation #2

- *The evaluation of the practice can be used as a criteria for meeting a chronic disease objective for the Primary Care Network*
 - There is no need for identifiable information to report against the defined objective, therefore a summary report will be developed which has no identifiable information.
 - A copy of the summary report and the detail report will be kept in a secure location for “x years” which supports audit and billing standards defined in the PCN agreement.

Variation #3

- *The data to perform the comparison is not available in the electronic medical record, but some billing information can be used as a proxy.*
 - Your analysis of the data indicates that the billing information was collected with a specific purpose and will not provide the required accuracy for the secondary use. You do not proceed with the secondary use.

5.2.2 Use Information of Another Family Member for the Direct Care of a Patient

Contemplated Secondary Use – you are treating a patient and want to access records of family members who are also your patients to determine if there is a higher risk for a patient due to hereditary factors.

1. Purpose & Categorized Use

The purpose is the treatment and care of family members and is a secondary use of the patient information. The records of the family are available to you as they are also patients in your practice.

The *Health Information Act* explicitly defines assembling a family history as an enabled purpose providing that the context is for providing health service to the family member.

2. Assessment of the ethical considerations

There is a clear differentiation of treatment or care based on family history. The condition itself is not overly sensitive and you don't believe that the family member would object to the use of the information. There is no need for disclosure of the actual condition or the details of the treatment to the patient being treated.

3. Consent model & oversight

The *Health Information Act* explicitly identifies that consent is not required. No oversight is required.

4. *Data and security controls*

N/A

Assessment – this is a legitimate secondary use with appropriate due diligence.

Variation #1

- *The history has significant social stigma and you feel the family member would not want any disclosure of the information.*
 - There is an ethical risk to the family member that disclosure of the historical condition violates their right to privacy. The legal duties to use the information in a limited manner and with the highest degree of anonymity possible are also heightened, therefore due consideration must be taken regarding the accessing of information as well as potential disclosure. You decide that the patient in care is at material risk and that the secondary use is justified. You access the information in private to ensure there is no accidental disclosure but do not disclose the information to the patient, nor use it as justification for the treatment.

Variation #2

- *The patient presents a concern that their spouse is being treated for a communicable disease. You know that there is marital discord. The spouse is not your patient, but you have access to the provincial EHR where you can access laboratory reports and establish the history.*
 - The patient shows no symptoms of the disease. You determine that the secondary use would not be ethical in these circumstances and do not access the records.

5.2.3 **Disclosing Information to Family Members**

Contemplated Secondary Use – you are treating a patient and want to share information with a family member regarding their care.

1. *Purpose & Categorized Use*

The purpose of the disclosure is to support the treatment and care of the family member. The disclosure is to an individual who is not the subject of that information therefore it is a secondary use of the patient information. The category of secondary use is legally permitted; therefore you require permission for this purpose.

2. *Assessment of the ethical considerations*

Absent the situation where the patient is not capable of caring for themselves, there should be respect for the personal privacy of the patient.

3. *Consent model & oversight*

Explicit consent is required. No oversight is required.

4. *Data and security controls*

N/A

5.2.4 Using Clinical Data to Populate the Provincial Electronic Health Record

Contemplated Secondary Use – new functionality has been added to the Provincial EHR that enables systematic uploading of patient data from your electronic medical record to the patient profile in the EHR. You are considering enabling the functionality in your electronic medical record which will begin posting of that information.

1. Purpose & Categorized Use

The purpose is direct care of the patient by other professionals. You will be posting data collected for the care and treatment of individual patients to assist physicians and authorized health care professionals to provide direct care to patients. There may be other disclosures resulting from the secondary use, but those uses are governed by the EHR.

The *Health Information Act* explicitly enables disclosures to electronic health records.

2. Assessment of the ethical considerations

There is a formal statement of endorsement from the College that the purposes encompassed in the Information Sharing Agreement are beneficial and there is an appropriate balance of risk and benefit. The governance model for changes to the Information Sharing Agreement is respectful of the secondary use principles published by the College. The information to be disclosed is limited to those providing direct care to the patient, and you are comfortable that the information will be contextually relevant for subsequent uses.

3. Consent model & oversight

The *Health Information Act* enables this disclosure with no consent requirement as the EHR has an oversight committee which has deemed the disclosure to be of benefit to patients and to the health system.

4. Data and security controls

The Information Sharing Agreement has detailed the access and secondary uses and there are binding terms in the agreement. You have evaluated your charting protocols and have determined that your electronic medical record can successfully and accurately post information to the EHR.

Assessment – this is a legitimate secondary use with appropriate due diligence.

Variation #1

- *There is no mechanism in the transfer process which allows for exceptions to the standard access privileges in the EHR. You have patients who have sensitive information and have explicitly requested non-disclosure. There are plans to incorporate a masking capability in some future release but there is no fixed date or schedule.*
 - You determine that the risk to the doctor-patient relationship outweighs the potential benefits of the EHR. You are also concerned that the College has not endorsed the transfer of information. You elect to defer participating until the masking capability has been implemented allowing you to respect your patient's expressed wishes.

5.2.5 Using Clinical Data to Research Treatment Outcomes

Contemplated Secondary Use – the Primary Care Network in which you practice has been engaging a nurse practitioner to assist in the treatment of “chronic disease”. You want to compare treatment outcomes from the previous year to outcomes from historical records to determine if the treatment has demonstrated improvements to health outcomes and is an appropriate use of the nursing resource.

1. *Purpose & Categorized Use*

The purpose of the research is for planning and resource allocation which is an explicitly defined purpose enabled by the *Health Information Act*. You require personally identifiable information to match outcomes from year to year but there will not be any personally identifiable information disclosed in the study which you will publish for the benefit of other Primary Care Networks.

2. *Assessment of the ethical considerations*

There are no external resources employed in this study and no planned disclosure of identifiable information. There is very limited risk to patients.

3. *Consent model & oversight*

The *Health Information Act* explicitly identifies that consent is not required. No oversight is required.

4. *Data and security controls*

Only summary non-identifiable information will be reported. All interim data stores will be password protected to ensure there is no inappropriate access to the information. The data itself will be archived in a secure location to provide a basis for on-going comparisons.

Assessment – this is a legitimate secondary use with appropriate due diligence.