# An Application of the Privacy Management Reference Model & Methodology (PMRM)

# to HL7 Consent Directive Use Cases

By
Christopher John Guinan

A Thesis Submitted to
Saint Mary's University, Halifax, Nova Scotia
in Partial Fulfillment of the Requirements for
the Degree of Master of Business Administration.

April, 2013, Halifax, Nova Scotia



Approved: Dr. Dawn Jutla
Professor & MRP Supervisor

Approved: Dr. Mark Raymond
Associate Dean, Masters Programs

Date: April 5, 2013

# Abstract

An Application of the Privacy Management Reference Model & Methodology (PMRM) to HL7 Consent Directive Use Cases

Christopher J. Guinan

April 5, 2013

The importance and sensitivity of personal health information has led to an increased focus on privacy protection measures as personal health records are digitized. Systems and legislation are rapidly adapting to meet both technology and consumer concerns. *An application of the Privacy Management Reference Model & Methodology (PMRM) to assess HL7 Consent Directive Use Cases* will provide policy makers, health care providers, and consenters alike the ability to assess the effectiveness of current practices when it comes to the interoperability and the protection of Individually Identifiable Health Information. A solid foundation will be provided to recommend how all stakeholders can work together to improve the consent processes, and ultimately improve the effectiveness of privacy protection measures as they relate to personal health information.

# Table of Contents

# Ch 1 – Introduction

Few things are as important to an individual as his or her health and wellness. Health is the catalyst for all one hopes to do and achieve in their life, and as a society healthcare consumes a significant portion of our resources. It is a source of considerable focus for both governments and individuals.

Privacy in the healthcare field is particularly important due to the highly personal nature of health records and the potential for unlawful misuse of health information to deny access to jobs and promotion opportunities. Privacy concerns and issues have only been heightened as the search for delivery improvements and efficiency has led to the digitization of health records. The reason for this digitization is quite straightforward: the aggregation and improved data flows for health care providers. This leads to greater consistency, accuracy and efficiency. The digitization of these records does, however, lead to increased concern-surrounding privacy, and who should have access to what data.

Governments have recognized the privacy implications of increased data sharing as technology evolves, and have created legislation to reflect this quickly evolving reality. However, as each jurisdiction is responsible for creating its own legislation the transmission of data across jurisdictional boundaries becomes complicated.

*1.1 - Objectives*

This paper will examine the patient consent process as it relates to the sharing of personal health records between health care providers in Nova Scotia, Canada. This analysis will be conducted using the methodology of the Privacy Management Resource Model (PMRM). The HL7 Use Case takes an in-depth look at the actors, systems, and processes involved in Privacy Consent Directives and will be reviewed through the PMRM lens. The analysis will reveal some of the strengths and weaknesses of the PMRM methodology. It will serve as the basis of further improvement of the methodology.

# Ch 2 - Literature Review

The impact of digitized health records has been the subject of increased study and scrutiny in recent years. The aggregation and improved information flows associated with the collection of massive amounts of sensitive health information has amplified concerns over privacy. While most agree this is a major step forward for the efficiency and accuracy of the vital data that researchers and health care professionals use to improve patient care, legitimate questions arise about how to strike the delicate balance between a patient's right to privacy and the provider's need for information. The impact of this debate is being felt legislatively, socially, and economically.

*2.1 – Legislation:*

Throughout Canada, there has been recognition on the part of governments and policy makers about the importance of, and right to, privacy protection in light of an increasingly digital environment. Therefore a Pan-Canadian Health Information Privacy and Confidentiality Framework was established among provincial and territorial leaders in order "to respond to Canadians' privacy and confidentiality expectations and to suggest a harmonized set of core provisions for the collection, use and disclosure of personal health information in both the publicly and privately funded sectors" (Health Canada, 2005, paragraph 2). As it is the provinces that administer health care in Canada, this cooperation underscores the importance of consistency and streamlined processes in this sector.

The United States Department of Health and Human Services came forth with *Standards for Privacy of Individually Identifiable Health Information.* Part of the Health Insurance Portability and Accountability Act of 1996, it set national standards for the protection of certain health information in regard to use and disclosure. “A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being” (Firouzan & McKinnon, 2004, p. 3). This legislation pertains to providers and clients, and sets forth very specific parameters around what type of information is covered and on what the information can be used on.

In Canada, the “gold standard” of personal health privacy legislation is considered to be Ontario’s Personal Health Information Protection Act (PHIPA) (Cavoukian, 2010 slide 1). First implemented in 2004, it was “the only health sector privacy legislation that was declared to be substantially similar to Canada’s federal private sector privacy legislation, *PIPEDA,* in 2005.” (Cavoukian, 2010 slide 7).

PHIPA establishes rules surrounding the collection, use, and disclosure of health information; codifies a client’s right to confidentiality and establishes accountability and remedies for breaches (Cavoukian, 2010 slide 6)). Where PHIPA differs is in its use of the “Circle of Care”. This represents a clarification surrounding the ability of health information custodians to share information for health care purposes.

This legislation has been widely reviewed and mimicked. For instance, the Government of New Brunswick created a task force on personal health information, which

recommended the implementation of legislation regarding personal health information, based principally on Ontario's PHIPA (Cavoukian, 2010, slide 11). In Nova Scotia, the Personal Health Information Act was announced in late 2009, and enacted in 2010. It brought together many different privacy protections that exist under the law into one document. In May of 2012, the Government of Nova Scotia brought amendments to the legislation to the floor of the House of Assembly. These changes will take effect in June 2013. Among them was the recognition of the "Circle of Care", acknowledging knowledgeable implied consent as a model for delivery. Other changes also included the ability to revoke consent; the implementation of a Review Officer; institution of a complaints policy; and enforcement measures for policy violators (Nova Scotia Personal Health Information Act, 2012).

This shows that Nova Scotia, while later than Ontario's "gold standard" legislation, is quickly catching up to an emerging consensus and adopting best practices from other jurisdictions.

To meet these legislative guidelines requires changes to administrative, technical, and physical processes and equipment (Firouzan et al. 2004, p6**)**. Part of this compliance process is clear and frequent communication with clients to ensure they know the necessity of the change; training employees for the new systems; and in larger institutions the hiring of a compliance officer is necessary. A 2004 study of healthcare facilities in Pennsylvania found that the majority of facilities were simply unable to meet the specified compliance timelines (Firouzan et al. 2004 p. 8). This shows that there remain

significant challenges both in terms of stakeholder buy-in and logistics in order to implement new systems and operations for digitization compliance. Ultimately, organizational support and commitment is a key plank in compliance, as employees better recognize the importance of the change, and they are more likely to prove the necessary resources (Johnson & Warkentin, 2008, p. 11).

*2.2 – Economic & sociotechnical challenges*

Appari and Johnson, in their publication *The Current State of Research* say that even though many of these regulations and frameworks have been in place for several years, there is still a lack of clarity surrounding them. Accordingly, this creates a greater threat of breach from within than from external threats. Simply put, employees do not understand the requirements. This is due, in part, to the economic and technical hurdles associated with more effective access controls. Moving forward, they suggest more collaboration is required between policy makers and stakeholder groups to increase interoperability and compliance.

This leads to the importance of effective system design, which is a dynamic process as technology continues to evolve rapidly. Improvements are always necessary to ensure compliance and improved information flows as well (Russ et al. 2011). Issues of flow and interoperability are necessary so the information can be transferred easily while meeting the privacy requirements (Heinze, Birkle, Köster & Bergh, 2011, p. 3). Much has been written about the need for consultation and stakeholder engagement, as the distinct goals of all groups need to be accounted for and factored into the design. Better and more

representative designs will create greater efficiency, compliance, and trust in the system. It is an ongoing effort.

In addition to regulatory compliance and system integrity, there is the issue of public trust and confidence in the disclosure of sensitive information. Publicizing individually identifiable health information could have social or economic implications for the client (Laric, Pitta & Katsanis, 2009, p. 1). That is, health issues and choices made by individuals, if made public or discovered by unauthorized stakeholders, could cause personal tension or duress in their respective communities or impact career prospects. For such reasons, it is natural that individuals like to protect privacy and have confidence in the systems put in place. Privacy policies are a known way to build trust, but it is vital that these agreements must be comprehendible by the patients. Overly technical, overwhelming policies serve to confuse patients and create more apprehension (Vail, Earp & Antón, 2008, p. 451). More emphasis must be placed on the consumers throughout the process to achieve buy-in and understanding of the implications.

*2.3 Standards to support privacy process implementations*

The move to digitize health information has led to the collaboration of many scholars and stakeholders to create standards that make the flow of information for accurate, efficient, and protected. These standards are incredibly complex and detailed, with an over-arching goal to incorporate all important aspects into an interoperable platform.

One such standard, Health Level 7 (HL7), refers to the movement to develop international interoperability standards for health information systems. In Canada, Canada Health Infoway represents HL7. An independent, government-funded organization that sets out to accelerate the digitization of health records across the country. Ultimately interoperability will increase access, efficiency and effectiveness of the healthcare system in Canada (Canada Health Infoway, 2005, p. 29).

Canada Health Infoway has also come forth with privacy and security requirements for electronic health records. These are intended to protect the privacy of the individual and also uphold the integrity, accessibility and interoperability of the system. This, of course, is a delicate balance. On one hand, excessive restrictions and limitations prevents the efficiency and effectiveness of the data flows, while too much information being made available to too many would violate privacy legislation and undermine public trust.

Another standard is known as the Healthcare Information Technology Standards Panel (HITSP), which also aims to improve and increase standardization efforts for technology in the field in the United States. It sets forth standards for stakeholders to follow to achieve its interoperability goals as well.

Operating under the mandate of the US Department of Health and Human Services, HITSP put forth recommendations surrounding the consent process as it relates to the use and disclosure of personal health information. Criteria determining the basis upon consent being granted are: provider roles, operation required for the data, purpose of use,

condition or state client is in, time period under which information can be used, and the context that it can be shared (Health Information Technology Standards Panel report, 2009, p. 21). All conformance guidelines for HITSP as they relate to consent process standards fit within the over-arching goal of interoperability.

While there are different standards and different organizations creating the frameworks, the underlying goal remains the same: the creation of systems and processes that achieve a level of interoperability that improves the level of care received by patients. The holistic view taken by these organizations upholds the ability to embed privacy and consent designs while maintaining functionality.

*2.4 - Models & Methodologies for embedding privacy in processes*

There is an emerging mindset that privacy should not only be respected and codified in legislation when it comes to the use of personal health information, but it should be a cornerstone of information systems and processes moving forward. Dr. Anne Cavoukian, Ontario's Information and Privacy Commissioner has championed the embedding of privacy processes, and her work on both the Privacy by Design framework and Privacy Impact Assessments has generated acclaim, and is becoming widely adopted.

Privacy by Design (PbD) is a framework which seeks to influence technology design, business practices, and physical infrastructure by embedding privacy protection at its core. Since its inception in the early 1990s it has generated a great deal of attention acclaim, and in 2010 PbD was recognized as a new global privacy standard by

International Data Privacy and Protection Commissioners (Cavoukian, 2010, s. 19). This results in these principles having great influence on policy frameworks around the world.

Dr. Cavoukian has said that technologies can either be used to protect privacy or erode it, and that's why such a framework and outlook is important to establish. At its core PbD holds 7 principles:

1. Proactive, not reactive & preventative not remedial
2. Privacy as a default setting
3. Privacy embedded into design
4. Full functionality: positive sum, not zero sum
5. End-to-end security: full life cycle protection
6. Visibility and transparency: keep it open
7. Respect for user privacy: keep it user centric

These principles are relevant and apply to multiple levels of stakeholders. As such, it seeks to "Build a culture of privacy" (Cavoukian, 2010, s. 22). This means it encourages organizations to look beyond mere compliance and toward a culture of trust with well-trained and respectful employees, that in order to be successful all stakeholders must embrace the importance of privacy and recognize all have an role to play in enhancing its safeguards.

Central to PbD is the concept of data minimization. This is both a policy and a mindset under which health care providers would operate on a "need to know basis". That is,

collecting only what information is relevant to the service provided, and the limitation of the disclosure and sharing of information if existing data will serve the intended purpose. Ultimately minimized data collection and flows are an important part of protecting the client's personal health information.

Dr. Cavoukian also writes about Privacy Impact Assessments (PIAs). A PIA is a risk analysis tool. It relates to the individual health information privacy stemming from new systems, technologies or practices.

PIAs serve as a way for health information custodians to assess how they are adhering to privacy regulations and legislation. The intent is to go beyond simple compliance, but to recognize the importance of privacy and be able to be aware of how changes may impact individual privacy before those changes occur. It features a lengthy questionnaire, which focuses on two areas: organizational privacy management practices and the information system and technology involved (Cavoukian, 2010 p. 1). It is not only the technical systems in place that are important, but also the organizational practices relating to information sharing and access that can have an impact on privacy. These criteria and questions were created by a group of former Information & Privacy Commissioners from Canada and abroad (Cavoukian, 2010, p. 6). These PIAs must be thorough and give a full account of the systems in place and the processes associated with the collection and use of personal health information.

Both the Privacy by Design framework and the Privacy Impact Assessments work in concert with each other to influence the embedding of privacy processes in health care systems and operations. These techniques serve as a starting point and assessment mechanism to ensure that privacy protection is at the forefront in healthcare, and can be bolstered as technology develops, not diminished.

*2.5 Consent process for the release of private health data*

The consent process is the point at which existing concerns about privacy and existing cognitive biases on the part of the clients converge with regulatory compliance and health information system design. It is the critical juncture of the process, where the client comes face-to-face with the systems and processes designed to protect his or her personal health information. This will frame the use and flow of this information moving forward.

According to Canada Health Infoway's Electronic Health Record (EHR) Privacy and Security Requirements document, "Laws may require express, implied or deemed consent for specific collections, uses and disclosures of PHI (personal health information)" (Canada Health Infoway, 2005, p. 24). Expressed consent is when it is made clear by the client, through a privacy consent directive or another means, where and when certain information can be utilized. Implied consent is when, through actions on the part of the client or through interactions with the health care provide, it becomes clear that the utilization of certain information is necessary. Finally, deemed consent is what providers are able to collect and transfer based on the legislation put in place by a given jurisdiction.

Of course, a new ethical standard is sought in these circumstances, and the HL7 guidelines regarding consent contain a number of privacy requirements to meet the specifications of the standard. They are as follows:

- Obtain knowledgeable consent: This is not only to meet legal requirements, but to reach a new ethical standard. This will have the patient fully aware of her/her rights to change and revoke certain aspects, and how information will flow.
- Record consent in Point of Service system (POS): These point of service systems are connected to electronic health records infrastructure, and accordingly the recording of consent would register in the system.
- Associate consent with Personal Health Information in Point of Service System: the transmission of the consent directives must happen in consistent form with the health records infrastructure.
- Record consent in health record infrastructure: the health records infrastructure must record consent directives in such a way that jurisdictional regulations can be applied.
- Associate consent directives with personal health information in electronic health infrastructure: In the processing of this data a connection between the PCD and personal health records must be maintained. Also, when violated, the infrastructure must be able to block transmission of data and notify user.
- Log application of consent directives: the health records infrastructure must be able to log when access is overridden or prohibited, and alert compliance officers within the organization.

- Implications of consent directives must be known: make patients/clients aware of the impact of limiting access to personal health records, like the locking or masking of personal health information.
- Maintain a record of substitute decision maker's identity
- Ensure there is no coerced consent: Authorization must not be a condition of service.

These processes involve both technical and operational aspects. The guidelines show how tight the parameters are becoming in order to uphold these important standards. Through stakeholder consultations, these requirements have been refined and improved upon. The consent process is a critical juncture for the privacy requirements to be upheld and refined. It forms the foundation upon which the ultimate success of privacy protection measures will ultimately be determined.

The state of digitizing health records, and the public confidence that is a must to underpin it, is rapidly evolving. While regulations and laws are now in place to protect privacy and provide clarity for acceptable uses of IIHI, the elements of system design, public trust, and compliance are far from settled. While there is a recognition by all parties and stakeholders that this is an involved and complex process, much still needs to be done to secure systems and information flows and to educate both the public and system users about the parameters. Only through collaboration and mutual understanding can these issues be meaningfully addressed.

# Ch 3 – Methodology

This project uses the international Organization for the Advancement of Structured Information Standards' (OASIS) Privacy Management Reference Model and Methodology (PMRM) to fully explicate the HL7 consent management process to all stakeholders (see Appendix A). Industry, consultants, academics, and other stakeholders have developed PMRM as a method to comprehend and assess privacy management cases, and select appropriate processes and services that support established privacy controls.

The establishment of the PMRM model comes at a time when personal information is increasingly found on networked and interconnected platforms. This information sharing across new platforms creates a complex regulatory environment due to the interconnectivity of the domains and jurisdictions. PMRM helps to wade through the complexity which results from inconsistent and conflicting regulations that occur across domains and leads to informed policy development and system design that will be both predictable and trusted by all stakeholders. Below is the PMRM conceptual model, located in appendix A, page 6.

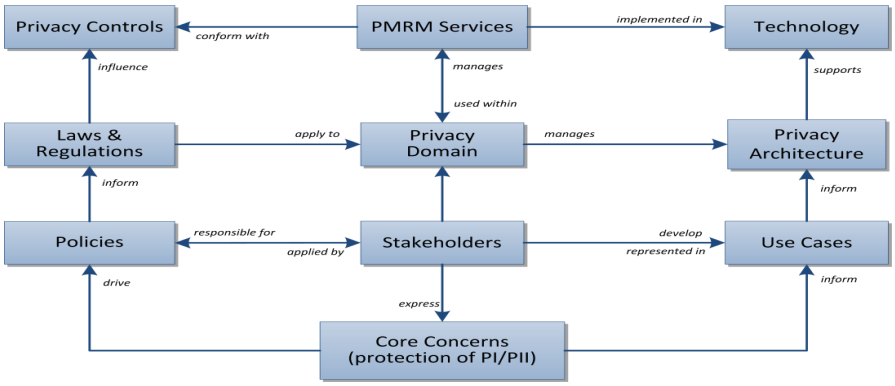


Figure 1. The PMRM Model. [Adopted from Sabo et al, 2012.]

The Privacy Management Analysis (PMA) and any Privacy Impact Assessments (PIA) that come out of applying PMRM help facilitate collaboration between all types of stakeholders: from system architects and developers, to policy makers and business owners. Ultimately, the results and analysis are applicable to all involved.

*3.1 – Analysis of use cases*

The PMRM methodology includes sections and tasks for the purpose of analyzing various use cases. When specifically applied to the HL7 Consent Directive Use Case, it will help assess its privacy consent processes. In PMRM, there are the following sections:

- Develop use case description and high-level privacy analysis
- Develop detailed privacy analysis
- Identify functional services necessary to support privacy controls
- Define the technical functionality and business processes supporting the selective services
- Perform risk and/or compliance assessment

- Initiate iterative process
- Operational definitions and glossary

Ultimately, PMRM is an important diagnostic tool, which established a framework from which to analyze privacy impacts in an increasingly complex and interconnected environment. By its very nature PMRM it is proactive. The analysis of use cases helps to uncover gaps in existing processes and feeds into risk management models, driving internal change in industries. At best, PMRM can influence changes in policy and implementation, and have a role in future developments in the protection of private or sensitive information.

*3.2 – Methodology limitations*

A major hurdle for privacy protection is public trust. As the Literature Review states, in order for the public and policy makers to have confidence in the system there needs to be broad-based consent and understanding. PMRM, while long and technical, is not reader friendly and does not directly address the need for strong public confidence in the systems put in place. This methodology needs to be crafted with the laymen in mind. After all, without fundamental understanding and collaboration it becomes difficult to make impactful changes to improve existing systems.

However, as privacy management is particularly important in healthcare, applying PMRM to consent processes in the HL7 use case will provide a good indication of what gaps exist in established processes to protect this very sensitive health information.

# Ch 4 –PMRM Analysis of the HL7 Consent Directive Use Cases

The sections below each represent a section of the Privacy Management Reference Model and Methodology. Throughout this chapter the use case and privacy analysis will be reviewed; functional support services will be identified; and a risk and compliance assessment will be conducted. Ultimately this will lead to a set of recommendations related to how and where HL7 can ultimately improve its processes to better protect and respond to privacy challenges.

## *4.1 - Develop Use Case Description and High-Level Privacy Analysis*

### *4.1.1 Application and business process descriptions*

Use case description

A non-profit organization, known as HL7 is dedicated to the development of international interoperability standards for health informatics. Participants in the HL7 organization provide a structure and platform for the "exchange, integration, sharing, and retrieval of electronic health information" (ANSI, 2013). HL7 works around the world with sanctioning bodies and standards developers to ultimately push for a supportive and compatible set of standards. This work has led to widespread acclaim and adoption of its standards.

The HL7 Consent Directive Use Cases are based on the 2008 recommendations from the American Health Information Community Consumer Empowerment Workgroup for the construction and utilization of privacy consent directives for individual health information (HL7, 2011, p. 1).

At its core, these Use Cases is underpinned by the principal recommendation that the functional and technical capabilities are in place to control the "collection, access, use, and disclosure of individually identifiable health information (IIHI)" (HL7, 2011, p. 3).

Use case inventory

The following are a list of the HL7 Consent Directive Use Cases that will be reviewed as part of the analysis:

- Grant control of the IIHI to Individuals
- Manage Privacy Consent Directives
- Provider System requests Privacy Consent Directive for a Client prior to disclosure
- Provider requests IIHI
- Information system masks Health Record Information based on Consumer preferences
- Information system flags masked Health Record information
- Provider amends IIHI based on consumer's Privacy Consent Directive
- Request privacy policies from organization or jurisdiction

- Provide electronic Privacy Consent Directive to a specific healthcare provider
- Patient provides verbal Privacy Consent at point of service
- Provider requests IIHI from another jurisdiction
- Request for pre-fetch of DI exams
- Provider override Privacy Consent Directive
- Accounting of disclosures (addressed PASS audit)

Systems: The Point of Service system (POS) that is connected to Health Record Information System used by providers that store electronic health records and disseminate information based on the specifications in place by the Privacy Consent Directive. A good example of the functions of a POS are given in Ontario's eHealth Consent Directive Implementation Guide Ver. 1.01 (Personal Health Information Protection Act, 2004). The POS would implement a consent management program responsible for consent directive management, enforcement, business, and technology operations. Consent management deals with creating, updating, deactivating, reinstating, and outputting patient directives. Enforcement covers, and is not limited to, application of patient consent rules, providing consent-related stakeholder notifications, administering temporary overrides (for example in emergency or mental health related situations), and obtaining consent status information. Technology operations refer to any function that supports the consent management solution, such as new lines of business integration, new technology integration, software process updates, technology performance monitoring and reporting. Examples of business operations, in the context of consent management, include policy

establishment and communication, change management, and business continuity processes in case of an online system failure.

Legal and Regulatory: Jurisdictional authorities provide the regulatory environment to grant, withdraw, or withhold privacy consent options. Regulations also set default policies and classifications that specify when restrictions on the use of individually identifiable health information (IIHI) are not required.

According to the Provincial Government, Nova Scotia's Personal Health Information Act, it sets out to "govern the collection, use, disclosure, retention, disposal, and destruction of personal health information in a manner that recognizes both the right of individuals to protect their personal health information and the need of custodians to collect, use, and disclose personal health information to provide support and manage health care". This includes penalties and fines for those who are not in compliance as determined by privacy officers (Personal Health Information Act, 2010).

Additionally, the privacy of Nova Scotians is protected by the Freedom of Information and Protection of Privacy (FOIPOP) Act. The FOIPOP Act establishes parameters when it comes to the collection, use, and disclosure of individual information by public bodies and municipalities. This includes hospitals and the work they do with universities for research purposes. Like the Personal Health Information Act, FOIPOP defines what is considered appropriate for the collection, use, and disclosure of personal information in the conduct of the day-to-day activities of public bodies and municipal units.

The work of upholding the FOIPOP Act falls to the Review Officer, Dulcie McCallum; as well as a team which includes a Director, an Investigator, a Portfolio Officer, and an Intake Analyst. After all, without the ability to enforce these guidelines, the laws themselves would be meaningless. To that end, based on the work conducted by the FOIPOP team is vital to uphold system integrity and public confidence.

To supplement the FOIPOP act, in 2006 the Nova Scotia Government passed the Personal Information International Disclosure Protection Act (PIIDPA), which extended protection and addressed concerns about foreign access and disclosure of the same information. PIIDPA prevents public bodies or municipalities from granting foreign access, sharing, or storing of personal information, unless necessary for the conduct of public duties. Violation of this Act carries with it substantial fines of up to $500,000.

It is important to have a legislative framework in place that keeps up with the increasingly complex and interconnected nature of today's data sharing, as well as providing an adequate penalty to ensure compliance. With FOIPOP, and in recent years the passage of the PHIA and PIIDPA, it is clear the Nova Scotia Government understands the importance of privacy protection and recognizes the challenges associated with maintaining the integrity of that important goal.

Customer: PCDs vary depending on regulatory environment in a given jurisdiction.

The customer is the patient or substitute decision maker. A substitute decision maker is someone (e.g. a parent of an underage child) who is authorized to consent on behalf of the

patient, to collection, use, or disclosure of the patient's personal health information.

*4.2 Applicable privacy policies*

Privacy policy conformance criteria

First, disclosure of IIHI must conform to existing guidelines put in place by the Nova Scotia's (or other province or territory in which data is collected) Personal Health Information Act. Each province or territory, through its respective legislation sets out exceptions to what can be subject to a client's Privacy Consent Directive, types of information that is not subject to the legislation.

There are instances where implied consent may prove sufficient for the collection and sharing of data, however. Implied consent occurs when the client or patient seeks out the assistance of medical professionals, and the collection and utilization of personal health information is required to conduct the service.

*4.3 Initial privacy impact or assessment*

Assessment preparation

Based on HL7's recommendation, personal health records should have the technical versatility to allow the consumer to specify conditions for the collection, access, and distribution of certain aspects of their health information.

That is, when a patient or consumer of health care services goes to a provider, they are able to agree on the parameters on future usage of information and data collected from that visit.

All of this must occur under the umbrella, however, of guidelines put in place by Nova Scotia's Personal Health Information Act as it relates to granting consent for the collection and use of the individually identifiable health information. In this case, Nova Scotia's PHIA states that consent can be expressed (through a PCD for example), implied, or deemed. In addition, consent can be revoked or limited and designated to others. It also puts limitations on the custodians of the data for how they implement these directives, for example it limits what can be collected to only what is necessary to receive the service, and if that could not be conducted using existing information. Other restrictions, such as encryptions prevent custodians from seeing information that is not relevant to the procedure. These ultimately determine the level of discretion the consumer has, and the level the provider can offer.

Leakage of personal health information to unauthorized parties outside the circle of care for a patient is a risk of any system. These unauthorized parties may be employees in a hospital, other health service providers, dentists and their employees, insurers and their employees, or external hackers. The consent directives themselves may contain personal information that should not be disclosed. Access to PHI can be socially engineered with or without the presence of a computerized system. As most systems are a combination of human and computer processes, they are vulnerable to human-based, computer-based, and hybrid attacks. Consent directives are at risk if they do not adhere to the principle of

data minimization.

*4.4 - Develop detailed privacy analysis*

*Identification of participants and systems, domains and domain owners, roles and responsibilities, touch points and data flows*

Identify participants

- Patients/clients crafting Privacy Consent Directives.
- Substitute decision makers for patients who are authorized to create, or modify consent directives
- Provincial Legislators in Nova Scotia who crafted and passed PHIA.
- Health care providers (and their appointed employees) who may access and use information in provision of care under implied consent
- Personal Health Information Requestor can be a system or user who requests PHI.
- Health Information System architects
- System administrators
- Privacy officers
- Jurisdictional authority
- Consent Registrar
- Personal Health Record Producer

Identify systems

- Point of Service system
- Consent directive management system (CDMS) and service
- Electronic Health Record Infrastructure – provider's information systems.
- Consent Requester

Identify privacy domains and owners

Two major types of privacy domains exist: consenter (patient or substitute decision maker), and health providers, In the circle of care, multiple privacy domains exist. That is each health care provider (e.g. physician, specialist, physiotherapist, dentist, etc) has its own privacy domain. Individuals have the right to put limitations on the collection, use, and sharing of IIHI. This level of consent can be adjusted or revoked (within the parameters set forth by Nova Scotia's PHIA). The personal health record repository is in the consenter's domain.

Providers: Point of service and provider information systems are put in place to ensure that the IIHI are protected as per the patient's PCD and within the broader regulations set forth by the Nova Scotia Government's PHIA. For now, we assume that the POS, HER, and the CDMS are in the same privacy domain, even though it would be more efficient, and less burdensome to the patient, to have a centralized CDMS to service all the distributed Points of Service. However, the latter is not in the state of the art section of this paper.

Identify roles and responsibilities within a domain

The system architects are responsible for creating the information systems responsible for protecting and effectively transferring the IIHI that operates within the regulations and PCDs put forward.

System administrators (custodians) are to be sure that consent directives and EHRs are accurate and up to date.

Consenters and Providers have the responsibility to know the framework that they operate in. Simply put, know their respective rights and responsibilities.

Identify touch points

The implementation of a client's Privacy Consent Directive into the Point of Service System; a Provider's request of IIHI; Amendments to IIHI based on changes to the PCD; and requests for IIHI from other jurisdictions are all points at which the data flows intersect with system and privacy domains.

A client requests to create, view, and maintain their consent directives occur at the interface of the client and the consent directive management system. This interface is a touch point. A client may grant temporary override privilege to access her/his PHI under certain circumstances. Such granting occurs at the same client-consent directive management system touch point. When notifications about consent directives are provided to the patients, other delivery touch points may come into play, for e.g. text,

email, snail mail, or telephone interfaces.

A touch point will also exist between the consent directive management system and the policy system. The policy system would include the organization's privacy and security policies management, including others for risk, audit etc. A further touch point is between a privacy officer and the consent directive management system. For example, the privacy officer may request reports on the management of patients' consent directives. Touch points also exist between the consent directive management system and the audit /logging/monitoring systems.

Suppose a client falls ill when traveling to another province or country. It is plausible then that personal health information may be shared between different jurisdictions. The two jurisdictions may have dissimilar consent directive management systems. There will be touch points between the two systems that would need to harmonize the disparity according to some prior agreements or legislation equivalence rules that translate to new privacy controls on the data.

Identify data flows

Data flows closely follow the touch points, or times when interfacing between clients, the system, providers, and policy systems occur.

Data flows from the client to the Privacy Consent Directive. From there, data flows between the PCD to the organization's policy system; from the policy system to the

client's personal health record. In addition, data flows from the provider to the personal health record, and in the transfer between providers. When such transfers occur, interfacing takes place with the PCD and the limitations placed on it by the systems.

### *4.4.1 - Identify PI in use case privacy domains and systems*

Identify incoming PI

Privacy Consent Directives provided by the client into the Provider's Information System, as well as the input of more IIHI to the client's Electronic Health Record.

Identify internally generated PI

Through client visits to the provider, additional information and data is generated for the Electronic Health Record. Consent directives may be changed as a result of any visit. New information may be generated through linking different data and generating a diagnosis for example.

Identify outgoing PI

Outgoing data occurs in the sending or transferring of Personal Health Records and IIHIs to Providers or other Jurisdictions when consent directives allow their release.

*4,4.2 - Specify required privacy controls associated with PI*

Specify inherited privacy controls

Regulations from Nova Scotia's Personal Health Information Act dictates the conditions around where and when consent can be granted. Once established, the Provider's Information System inherits privacy controls associated with the client's Privacy Consent Directives. This establishes the conditions and restrictions upon which the provider can access, collect, use, or disclose the client's Individually Identifiable Health Information (IIHI) within the client's Personal Health Records (PHR).

Specify internal privacy controls

Internal privacy controls are largely dictated by existing regulations put in place by Nova Scotia's Personal Health Information Act. In most cases these are a convergence of best practices among policy makers.

Examples of these internal privacy controls are over-arching codes of conduct put in place by the providers, which largely follow laws and regulations put in place by the jurisdictional authority, in this case it would be the Nova Scotia Government's Personal Health Information Act. In addition, the systems that the providers have to manage and control data must contain safeguards to protect privacy and uphold the client's PCD.

Specify exported privacy controls

Exported privacy controls come into play when sending Personal Health Records to other providers, and in some cases in other jurisdictions. The extent of the information contained in the Personal Health Record will be subject to the restrictions implemented by the client in the Privacy Consent Directive. Certain information may be masked based on the restrictions placed on the IIHI by the client, and then the filtered information is sent to the information requesters. The consent directive itself is thus an exported privacy control.

*4.5 - Identify functional services necessary to support privacy controls*

*Services needed to implement the controls*

Identify the Services necessary to support operation of identified privacy controls

Based on Incoming and Outgoing PI:

Establishment of Privacy Consent Directive – the client establishes PCD by specifying restrictions on use of Personal Health Records. To make changes to the PCD, an Authenticated customer identity and Keywords need to be established in the system by the client.

Accessing Personal Health Records – whether sent between providers or accessed

internally, information is encrypted when sent between providers or between jurisdictions. These access filter systems prevent certain information from being seen (cryptographically protected) by those not authorized by the Privacy Consent Directive.

Thus security services, including identity management, authorization and encryption for both storage and transmission of PHI are essential. In addition, at minimum, audit, enforcement, notification, and usage services are also needed.

*4.6 - Define the technical functionality and business processes supporting the selected services*

*Identify Functions Satisfying the Selected Services*

Identify the Functions that satisfy the selected Privacy Services

The establishment or alteration of Privacy Consent Directive requires communication between the Provider's Information System and Point of Service system that stores information on keywords entered by client to authorize changes.

The PHRs accessed and transmitted by providers are encrypted to protect information specified in the client's Privacy Consent Directive.

*4.7 - Perform Risk and/or Compliance Assessment*

Conduct risk assessment: a small example

Penalties for breaches under the Nova Scotia Personal Health Information Act (PHIA) vary depending on whether it is an individual or corporation in violation, or what type of violation occurs. These penalties can either come in the form of jail time of up to $10,000 and 6 months in prison for an individual, and up to a $50,000 fine for a corporation. Ultimately, the Courts will decide on the severity of the penalty based on its interpretation of the situation (Personal Health Information Act, 2010). Therefore, the risk incurred by providers and corporations that access data is that jail time or fines may be incurred if they do not take sufficient steps to protect privacy and respect existing guidelines.

FOIPOP is another piece of legislation that applies to hospitals and also has penalties for privacy violations that occur as a result of poor management. Finally violation of the Personal Information International Disclosure Protection Act (PIIDPA) carries with it substantial fines of up to $500,000. These penalties imply that medical service providers need to have sophisticated privacy mechanisms in place, including state-of-the-art security systems to prevent unauthorized transmittal of data. If not, the access and transmission of encrypted PHRs or EHRs could be *compromised.*

*If the PCDs are not current* based on the refinement of specifications made by the client, it is possible that the system will leak information that is not in accordance with patients' consent directives and expectations. A proper risk assessment should be conducted using a methodology such as Carnegie Mellon's OCTAVE (Operationally Critical Threat,

Asset, and Vulnerability Evaluation) tool suite.

# Ch 5 – Findings of PMRM Analysis on Consent Directives

The PMRM analysis on the consent processes associated with the collection, use, access and disclosure of individually identifiable health information provided a thorough analysis of the actors, systems, roles, responsibilities, functions, and vulnerabilities of the process outlined in the HL7 Consent Directive Use Case. From this, conclusions can be drawn on a larger scale and shed light on what still needs to be done to further protect and enhance privacy processes.

Broadly speaking, the Privacy Consent Directive process is a vital step in the establishment of public recognition and understanding of how individuals' personal health information is used and shared. Without it, those who advocate for the protection of privacy and seek to enhance existing regulations and systems are simply doing so on a conceptual basis. Without client interaction or direct involvement it becomes hard to generate public support or lobby effectively. It takes an understanding of relevant actors, data flows, and system specifications to truly understand how effectively (or ineffectively) personal information is being protected. By putting the onus on the public to specify his or her own Privacy Consent Directives, more attention is put on this important subject.

The PMRM analysis did an effective job of outlining the technical processes associated with Consent Directive Management Systems. That is, the flow of data between

consenters and providers, between providers, and between jurisdictions. It is ultimately a matter of the system integrity that will determine how effective the safeguards like authenticated consumer identities and encryptions are. That is a difficult question to answer with the PMRM analysis, and one better posed to computer scientists and system engineers. The dynamic nature of technological develop assures us, however, that newer more powerful, efficient and secure systems will be within reach in future.

Another element of the Privacy Consent process that showed through in the analysis was the complicating role played by jurisdictional authorities. As one of the main actors in PMRM, the jurisdictional authorities (regulating bodies & governments) had different privacy policies as they relate to individually identifiable health information. This makes the transmission of data between providers and clients in different jurisdictions complicated and uncertain. With different definitions and interpretations of what can be contained within a Privacy Consent Directive, it makes it difficult for clients to understand and more complex for systems to protect certain information when data flows between jurisdictions. This proved a glaring area for future work to take place in order to streamline the processes in an increasingly integrated health environment.

The over-arching goal for all stakeholders involved in the protection of personal health data should be the same: to simplify and protect the systems responsible for the collection and transmission of individually identifiable health information. It is safe to say this goal is a work in progress. From a legislative and technological standpoint, developments will

continue to smooth out the wrinkles that currently exist within the process. It underscores the importance of all stakeholders coming together to ensure that those sharing common goals can pull in the same direction, as it is a multifaceted approach to the simplifying and strengthening these systems so privacy protection can continue to be enhanced.

The PMRM analysis was effective at aggregating the relevant players and issues associated with the Privacy Consent Directives outlined in the HL7 use case. These conclusions provide good insight into the issues and vulnerabilities faced in the protection of personal health information, and can be used to direct further research and analysis on the matter.

# Ch 6 – Summary

The digitization of health records put increased scrutiny on the issue of privacy management in healthcare. While leading to improvements in the aggregation, efficiency, and accuracy of data flows, the issue of how best to balance personal discretion and access is still far from settled.

There are many stakeholders involved in the digitization of health records and all need to do a better job coming together to ensure systems and regulations match. Interoperability needs to be at the core of future efforts to improve delivery. This means that health care providers and governments need to work together to ensure that uniform standards are put in place and existing silos are eliminated. This is not only required from a data flow perspective, but as costs pressures continue to rise governments will be forced to look more closely at regional cooperation in delivery.

The dynamic nature of technological development will mean that moving forward the focus should continue to be on the simplification and increased effectiveness of security mechanisms associated with new technology. Provider Information Management Systems will have to focus on improving technologies with those two goals in mind.

*6.1 – Future work*

As interoperability is a key element of privacy management in healthcare, the attention of future works should be focused on efforts at synchronizing legislation and systems related to the privacy of personal health records.

The PMRM analysis does not allow for in-depth comparison or review of competing health information management systems. Without specifications or a comparison of competing systems provided in the HL7 use case, it is difficult to look into privacy protection from a technical basis. A look into technologies associated with privacy protection would be valuable moving forward, particularly due to the fast paced evolution of data sharing technologies in the 21st century.

There is still work to be done to improve privacy protection, particularly as it relates to personal health records. Further analysis of the technological and regulatory environments would strengthen the overall analysis of the current state of privacy management in healthcare.

# References

Anderson, C.L. & Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Information Systems Research*, 22(3), 469-490. doi: 10.1287/isre.1100.0335

Babad, Y. & Lubitch, A. (2011). Ethical and Legal Issues of Privacy and Patient Rights in the Application of Information Healthcare Delivery Systems. *International Journal of Healthcare Technology and Management,* 12(3-4), 230-249. doi: 10.150/IJHTM.2011.040477

Bergmann, J., Bott, O. J., Pretschner, D. P. & Haux, R. (2006). An e-consent-based Shared EHR System Architecture for Integrated Healthcare Networks. *International Journal of Medical Informatics*, *76*(2-3), 130-136. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/16971171

Brown, P.F., Janssen G., Jutla, D., Magnuson, G., McNabb, J., Sabo, J., … Willet, M. (2012, October 31). *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0

Canada Health Infoway. (2005, February 7). *Electronic Health Record (HER) Privacy and Security Requirements: Reviewed with Jurisdictions and Providers,* Version 1.1

Cavoukian, A. (2010). *PHIPA: A World Leader, Privacy by Design- The Gold Standard* [Presentation Slides]

Cooper, T. & Collman, J. (2005). Managing Information Security and Privacy in Healthcare Data Mining. *Medical Informatics* (pp. 95-137). Retrieved from http://ai.arizona.edu/mis596a/book_chapters/medinfo/Chapter_04.pdf

Damschroder, L.J., Pritts, J.L., Neblo, M.A., Kalarickal, J., Creswell, J.W. & Hayward, R.A. (2007). Patients, Privacy and Trust: Patients' Willingness to Allow Researchers to Access Their Medical Records. *Social Science and Medicine*, 64(1), 223-235. doi: 10.1016/j.socscimed.2006.08.045

Firouzan, P.A. & McKinnon, J. (2004). HIPAA Privacy Implementation Issues in Pennsylvania Health Care Facilities. *Perspectives in Health Information Management,* 1 (3). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2047323/

Fisher, F. & Madge, B. (1996). Data Security and Patient Confidentiality: The Manager's Role. *International Journal of Bio-Medical Computing*, 43(1-2), 115-119. doi: 10.1016/S0020-7101(96)01236-6

Galpottage, P.A.B. & Norris, A.C. (2005). Patient Consent Principles and Guidelines for e-Consent: A New Zealand Perspective. *Health Informatics Journal,* 11(1), 5-18. doi: 10.1177/1460458205050681

Health Canada. (2005). *Pan-Canadian Health Information Privacy and Confidentiality Framework.* Retrieved from http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php

Health Level Seven. (2011). Consent Directive Use Cases. Retrieved from http://wiki.hl7.org/index.php?title=Consent_Directive_Use_Cases

Heinze, O., Birkle, M., Köster, L. & Bergh, B. (2011). Architecture of a Consent Management Suite and Integration into IHE-based Regional Health Information Networks. *Bio Med Central Medical Informatics and Decision Making*, 11(58). doi: 10.1186/1472-6947-11-58

Hoeyer, K. (2009). Informed Consent: The Making of a Ubiquitous Rule in Medical Practice. *Organization,* 16(2), 267-288. doi: 10.1177/1350508408100478

Johnson, M.E. & Appari, A. (2010). Information Security and Privacy in Health care: Current State of Research. *International Journal of Internet and Enterprise Management,* 6(4). Retrieved from http://digitalstrategies.tuck.dartmouth.edu/research/academic-

publications/information-security-risk-and-privacy-in-healthcare-current-state-of-resear

Johnston, A.C. & Warkentin, M. (2008). Information Privacy Compliance in the Healthcare Industry. *Information Management and Computer Security,* 16 (1). Retrieved from http://thecenter.uab.edu/media/2011/12/Information-privacy-compliance-in-the-healthcare-industry.pdf

Laric, M.V., Pitta, D.A. & Katsanis, L.P. (2009). Consumer Concerns for Healthcare Information Privacy: A Comparison of US and Canadian Perspectives. *Research in Healthcare Financial Management,* 12(1). Retrieved from http://www.thefreelibrary.com/Consumer+concerns+for+healthcare+information+privacy%3A+a+comparison+of...-a0208588735

Lederman, R. (2005). Managing Hospital Databases: Can Large Hospitals Really Protect Patient Data?. *Health Informatics Journal,* 11(3), 205-214. doi: 10.1177/1460458205055685

McClanahan, K. (2008). Balancing Good Intentions: Protecting the Privacy of Electronic Health Information. *Bulletin of Science, Tehcnology and Society,* 28(1), 69-79. doi: 10.1177/0270467607311485

Muldoon, J.D. & Sardinas, J.L. (1996). Confidentiality, Privacy and Restrictions for Computer-based Patient Records. *Hospital Topics,* 74(3). Retrieved from http://smu.worldcat.org/title/confidentiality-privacy-and-restrictions-for-computer-based-patient-records/oclc/121458943&referer=brief_results

Russ, A.L., Saleem, J.J., Justice, C.F., Woodward-Hagg, H., Woodbridge, P.A. & Doebbeling, B.N. (2010). Electronic Health Information in Use: Characteristics that Support Employee Workflow and Patient Care. *Health Informatics Journal,* 16(4), 287-305. doi: 10.1177/1460458210365981

Security, Privacy and Infrastructure Domain Technical Committee. (2009, July 8). *Health Information Technology Standards Panel: Manage Consent Directives Transaction Package*, Version 1.3.

United States Department of Health and Human Services. (2003, May). *Summary of the HIPAA Privacy Rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Vail, M. W., Earp, J.B. & Antón, A. I. (2008). An Empirical Study of Consumer Perceptions and Comprehension of Website Privacy Policies. *IEEE Transactions on Engineering Management,* 55(3). Retrieved from ftp://163.25.117.117/gyliao/PaperCollection/20100211/An%20Empirical%20Study

%20of%20Consumer%20Perceptions%20and%20Comprehension%20of%20Web%20Site%20Privacy%20Policies.pdf

Zickmund, S.L., Hess, R., Bryce, C.L., McTigue, K., Olshansky, E., Fitzgerald, K. & Fischer, G.S. (2008). Interest in the Use of Computerized Patient Portals: Role of the Provider-Patient Relationship. *Journal of General Internal Medicine*, 23(1), 20-26. doi: 10.1007/s11606-007-0273-6

# Appendix A

## Privacy Management Reference Model and Methodology (PMRM) Version 1.0

### Working Draft 05 – Edits to CSPRD01 of 12 April 2012

### 31 October 2012

**Technical Committee:**
OASIS Privacy Management Reference Model (PMRM) TC

**Chairs:**
John Sabo (john.annapolis@verizon.net), Individual
Michael Willett (mwillett@nc.rr.com), Individual

**Editors:**
John Sabo (john.annapolis@verizon.net), Individual
Michael Willett (mwillett@nc.rr.com), Individual
Peter F Brown (peter@peterfbrown.com), Individual
Dawn N Jutla (dawn.jutla@smu.ca), Saint Mary's University

**Abstract:**
The Privacy Management Reference Model and Methodology (PMRM, pronounced "pim-rim") provides a model and a methodology for:

- understanding and analyzing privacy policies and their privacy management requirements in defined use cases; and
- selecting the technical services which must be implemented to support privacy controls.

It is particularly relevant for use cases in which personal information (PI) flows across regulatory, policy, jurisdictional, and system boundaries.

**Status:**
This Working Draft (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or approved as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document Approval Process begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

# Table of Contents

# 1 Introduction

The Privacy Management Reference Model and Methodology (PMRM) addresses the reality of today's networked, interoperable capabilities, applications and devices and the complexity of managing personal information (PI)[1] across legal, regulatory and policy environments in interconnected domains. It is a valuable tool that helps improve privacy management and compliance in cloud computing, health IT, smart grid, social networking, federated identity and similarly complex environments where the use of personal information is governed by laws, regulations, business contracts and operational policies, but where traditional enterprise-focused models are inadequate. It can be of value to business and program managers who need to understand the implications of privacy policies for specific business systems and to help assess privacy management risks.

The PMRM is neither a static model nor a purely prescriptive set of rules (although it includes characteristics of both), and implementers have flexibility in determining the level and granularity of analysis required by a particular use case. The PMRM can be used by systems architects to inform the development of a privacy management architecture. The PMRM may also be useful in fostering interoperable policies and policy management standards and solutions. In many ways, the PMRM enables "privacy by design" because of its analytic structure and primarily operational focus.

## 1.1 Context

Predictable and trusted privacy management must function within a complex, inter-connected set of networks, systems, applications, devices, data, and associated governing policies. Such a privacy management capability is needed both in traditional computing and in cloud computing capability delivery environments. A useful privacy management capability must be able to establish the relationship between personal information ("PI") and associated privacy policies in sufficient granularity to enable the assignment of privacy management functionality and compliance controls throughout the lifecycle of the PI. It must also accommodate a changing mix of PI and policies, whether inherited or communicated to and from external domains or imposed internally. It must also include a methodology to carry out a detailed, structured analysis of the application environment and create a custom privacy management analysis (PMA) for the particular use case.

## 1.2 Objectives

The PMRM is used to analyze complex use cases, to understand and implement appropriate operational privacy management functionality and supporting mechanisms, and to achieve compliance across policy, system, and ownership boundaries. It may also be useful as a tool to inform policy development.

Unless otherwise indicated specifically or by context, the use of the term 'policy' or 'policies' in this document may be understood as referencing laws, regulations, contractual terms and conditions, or operational policies associated with the collection, use, transmission, storage or destruction of personal information or personally identifiable information.

While serving as an analytic tool, the PMRM can also aid the design of a privacy management architecture in response to use cases and as appropriate for a particular operational environment. It can also be used to help in the selection of integrated mechanisms capable of executing privacy controls in line with privacy policies, with predictability and assurance. Such an architectural view is important, because business and policy drivers are now both more global and more complex and must thus interact with many loosely-coupled systems.

[1] There is a distinction between 'personal information' (PI) and 'personally identifiable information' (PII) – see Glossary. However, for clarity, the term 'PI' is generally used in this document and is assumed to cover both. Specific contexts do, however, require that the distinction be made explicit.

In addition, multiple jurisdictions, inconsistent and often-conflicting laws, regulations, business practices, and consumer preferences, together create huge barriers to online privacy management and compliance. It is unlikely that these barriers will diminish in any significant way, especially in the face of rapid technological change and innovation and differing social and national values, norms and policy interests.

It is important to note that agreements may not be enforceable in certain jurisdictions. And a dispute over jurisdiction may have significant bearing over what rights and duties the Participants have regarding use and protection of PI. Even the definition of PI will vary. The PMRM attempts to address these issues. Because data can so easily migrate across jurisdictional boundaries, rights cannot be protected without explicit specification of what boundaries apply.

The Privacy Management Reference Model and Methodology therefore provides policymakers, program and business managers, system architects and developers with a tool to improve privacy management and compliance in multiple jurisdictional contexts while also supporting capability delivery and business objectives. In this Model, the controls associated with privacy (including security) will be flexible, configurable and scalable and make use of technical mechanisms, business process and policy components. These characteristics require a specification that is policy-configurable, since there is no uniform, internationally-adopted privacy terminology and taxonomy.

Analysis and documentation produced using the PMRM will result in a Privacy Management Analysis (PMA) that serves multiple Stakeholders, including privacy officers and managers, general compliance managers, and system developers. While other privacy instruments, such as privacy impact assessments ("PIAs"), also serve multiple Stakeholders, the PMRM does so in a way that is somewhat different from these others. Such instruments, while nominally of interest to multiple Stakeholders, tend to serve particular groups. For example, PIAs are often of most direct concern to privacy officers and managers, even though developers are often tasked with contributing to them. Such privacy instruments also tend to change hands on a regular basis. As an example, a PIA may start out in the hands of the development or project team, move to the privacy or general compliance function for review and comment, go back to the project for revision, move back to the privacy function for review, and so on. This iterative process of successive handoffs is valuable, but can easily devolve into a challenge and response dynamic that can itself lead to miscommunication and misunderstandings.

The output from using the PMRM, in contrast, should have direct and ongoing relevance for all Stakeholders and is less likely to suffer the above dynamic. This is because it should be considered as a "boundary object," a construct that supports productive interaction and collaboration among multiple communities. Although a boundary object is fully and continuously a part of each relevant community, each community draws from it meanings that are grounded in the group's own needs and perspectives. As long as these meanings are not inconsistent across communities, a boundary object acts as a shared yet heterogeneous understanding. The PMRM process output, if properly generated, constitutes just such a boundary object. It is accessible and relevant to all Stakeholders, but each group takes from it and attributes to it what they specifically need. As such, the PMRM can facilitate collaboration across relevant communities in a way that other privacy instruments often cannot.

## 1.3 Target Audiences

The intended audiences of this document and expected benefits to be realized include:

- **Privacy and Risk Officers** will gain a better understanding of the specific privacy management environment for which they have compliance responsibilities as well as detailed policy and operational processes and technical systems that are needed to achieve their organization's privacy compliance;
- **Systems/Business Architects** will have a series of templates for the rapid development of core systems functionality, developed using the PMRM as a tool.
- **Software and Service Developers** will be able to identify what processes and methods are required to ensure that personal data is created and managed in accordance with requisite privacy provisions.
- **Public policy makers and business owners** will be able to identify any weaknesses or shortcomings of current policies and use the PMRM to establish best practice guidelines where needed.

## 1.4 Specification Summary

The PMRM consists of:

- A conceptual model of privacy management, including definitions of terms;
- A methodology; and
- A set of operational services,

together with the inter-relationships among these three elements.

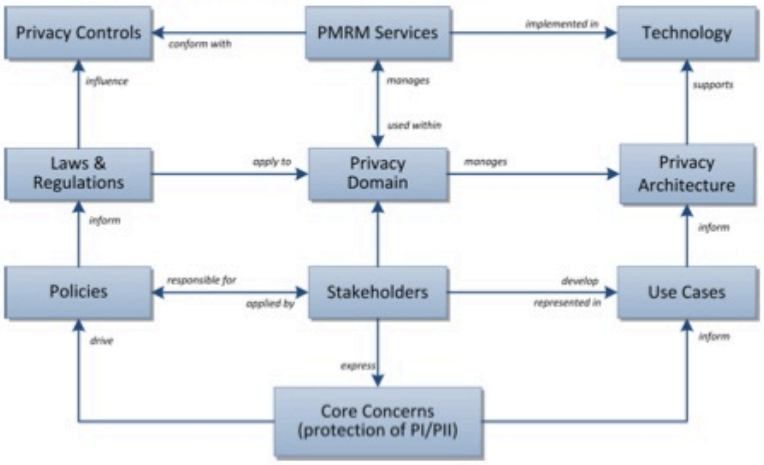


*Figure 1 – The PMRM Conceptual Model*

In Figure 1, we see that the core concern of privacy protection, is expressed by Stakeholders (including data subjects, policy makers, solution providers, etc.) who help, on the one hand, drive policies (which both reflect and influence actual regulation and lawmaking); and on the other hand, inform the use cases that are developed to address the specific architecture and solutions required by the Stakeholders in a particular domain.

Legislation in its turn is a major influence on privacy controls – indeed, privacy controls are often expressed as policy objectives rather than as specific technology solutions – and these form the basis of the PMRM Services that are created to conform to those controls when implemented.

The PMRM conceptual model is anchored in the principles of Service-Oriented Architecture (and particularly the principle of services operating across ownership boundaries). Given the general reliance by the privacy policy community on non-uniform definitions of so-called "Fair Information Practices/Principles" (FIP/Ps), a non-normative, working set of *operational* privacy definitions (see section 8.1) is used to provide a foundation for the Model. With their operational focus, these working definitions are not intended to supplant or to in any way suggest a bias for or against any specific policy or policy set. However, they may prove valuable as a tool to help deal with the inherent biases built into current terminology associated with privacy and to abstract their operational features.

The PMRM methodology covers a series of tasks, outlined in the following sections of the document, concerned with:

- defining and describing use-cases;
- identifying particular business domains and understanding the roles played by all Participants and systems within that domain in relation to privacy issues;
- identifying the data flows and touch-points for all personal information within a privacy domain;
- specifying various privacy controls;
- mapping technical and process mechanisms to operational services;

- performing risk and compliance assessments.

The specification also defines a set of Services deemed necessary to implement the management and compliance of detailed privacy requirements within a particular use case. The Services are sets of functions which form an organizing foundation to facilitate the application of the model and to support the identification of the specific mechanisms which will be incorporated in the privacy management architecture appropriate for that use case. The set of operational services (Agreement, Usage, Validation Certification, Enforcement, Security, Interaction, and Access) is described in Section 4 below.

The core of the specification is expressed in two normative sections: the High Level Privacy Analysis and the Detailed Privacy Management Reference Model Description. The Detailed PMRM Description section is informed by the general findings associated with the High Level Analysis. However, it is much more detail-focused and requires development of a use case which clearly expresses the complete application and/or business environment within which personal information is collected, communicated, processed, stored, and disposed.

It is also important to point out that the model is not generally prescriptive and that users of the PMRM may choose to adopt some parts of the model and not others. However, a complete use of the model will contribute to a more comprehensive privacy management architecture for a given capability or application. As such, the PMRM may serve as the basis for the development of privacy-focused capability maturity models and improved compliance frameworks. The PMRM provides a model foundation on which to build privacy architectures.

Use of the PMRM by and within a particular business domain and context (with a suitable Use Case), will lead to the production of a Privacy Management Analysis (PMA). An organization may have one or more PMAs, particularly across different business units, or it may have a unified PMA. Theoretically, a PMA may apply across organizations, states, and even countries or other geo-political regions.

Figure 2 below shows the high-level view of the PMRM methodology that is used to create a PMA. Although the stages are numbered for clarity, no step is an absolute pre-requisite for starting work on another step and the overall process will usually be iterative. Equally, the process of establishing an appropriate privacy architecture, and determining when and how technology implementation will be carried out, can both be started at any stage during the overall process.

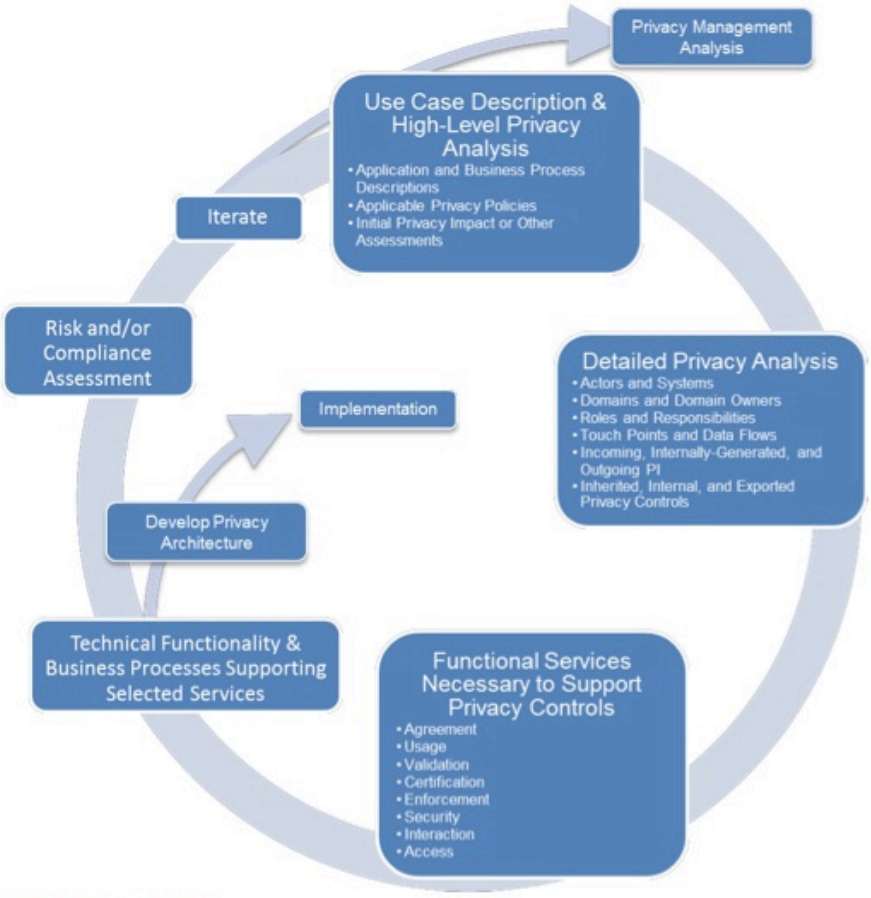


*Figure 2 - The PMRM Methodology*

## 1.5 Terminology

References are surrounded with [square brackets] and are in **bold** text.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **[RFC2119]**.

A glossary of key terms used in this specification as well as operational definitions for sample Fair Information Practices/Principles ("FIP/Ps") are included in Section 8 of the document. We note that words and terms used in the discipline of data privacy in many cases have meanings and inferences associated with specific laws, regulatory language, and common usage within privacy communities. The use of such well-established terms in this specification is unavoidable. However we urge readers to consult the

definitions in the glossary and clarifications in the text to reduce confusion about the use of such terms within this specification.

## 1.6 Normative References


**[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.


## 1.7 Non-Normative References


**[SOA-RM]** OASIS Standard, "Reference Model for Service Oriented Architecture 1.0", 12 October 2006. http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

**[SOA-RAF]** OASIS Specification, "SOA Reference Architecture Foundation 1.0" {Pending Designated Cross-Reference}

**[NIST 800-53]** "Security and Privacy Controls for Federal Information Systems and Organizations – Appendix J: Privacy Controls Catalog", NIST Special Publication 800-53 Draft Appendix J, July 2011.

# 2 Develop Use Case Description and High-Level Privacy Analysis

The first phase in applying the PMRM methodology requires the scoping of the application or business service in which personal information (PI) is associated - in effect, identifying the complete environment in which the application or capabilities where privacy and data protection requirements are applicable. The extent of the scoping analysis and the definitions of "application" or "business capability" are set by the Stakeholders using the PMRM within a particular domain. These may be defined broadly or narrowly, and may include lifecycle (time) elements.

The high level analysis may also make use of privacy impact assessments, previous risk assessments, privacy maturity assessments, compliance reviews, and accountability model assessments as determined by domain Stakeholders. However, the scope of the high level privacy analysis (including all aspects of the capability or application under review and all relevant privacy policies) must correspond with the scope of the second phase, covered in Section 3, "Detailed Privacy Use Case Analysis", below.

## 2.1 Application and Business Process Descriptions

### Task #1: Use Case Description

**Objective** Provide a general description of the Use Case.

**Example**

A California utility, with a residential customer base with smart meters installed, wants to promote the increased use of electric vehicles in its service area by offering significantly reduced electricity rates for nighttime recharging of vehicle battery. The system also permits the customer to use the charging station at another customer's site [such as at a friend's house] and have the system bill the vehicle owner instead of the customer whose charging station is used.

This Use Case involves utility customers who have registered with the utility to enable EV charging (EV customer). An EV customer plugs in the car at her residence and requests "charge at cheapest rates". The utility is notified of the car's presence, its ID number and the approximate charge required (provided by the car's on board computer). The utility schedules the recharge to take place during the evening hours and at times determined by the utility (thus putting diversity into the load).

The billing department calculates the amount of money to charge the EV customer based on EV rates and for the measured time period.

The same EV customer drives to a friend's home (also a registered EV customer) and requests a quick charge to make sure that she can get back home. When she plugs her EV into her friend's EV charger, the utility identifies the fact that the EV is linked to a different customer account than that of the site resident, and places the charging bill on the correct customer's invoice.

The billing department now calculates the amount of money to invoice the customer who owns the EV, based on EV rates and for the measured time period.

The utility has a privacy policy that incudes selectable options for customers relating to the use of PI and PII associated with location and billing information, and has implemented systems to enforce those policies.

### Task #2: Use Case Inventory

**Objective** Provide an inventory of the capabilities, applications and policy environment under review at the level of granularity appropriate for the analysis covered by the PMRM and define a High Level Use Case which will guide subsequent analysis. In order to facilitate the analysis described in the Detailed Privacy Use Case Analysis in Section 4, the components of the Use Case Inventory should align as closely as possible with the components that will be analyzed in the corresponding detailed use case analysis.

**Context** The inventory can include applications and business processes; products; policy environment; legal and regulatory jurisdictions; systems supporting the capabilities and applications; data; time; and other factors Impacting the collection, communication, processing, storage and disposition of PI. The inventory should also include the types of data subjects covered by the use case together with specific privacy options (such as policy preferences, privacy settings, etc. if these are formally expressed) for each type of data subject.

**Example**

Systems: Utility Communications Network, Customer Billing System, EV On Board System…

Legal and Regulatory Jurisdictions:

California Constitution, Article 1, section 1 gives each citizen an "inalienable right" to pursue and obtain "privacy."

Office of Privacy Protection - California Government Code section 11549.5.

Automobile "Black Boxes" - Vehicle Code section 9951.

…

Personal Information Collected on Internet:

Government Code section 11015.5. This law applies to state government agencies…

The California Public Utilities Commission, which "serves the public interest by protecting consumers and ensuring the provision of safe, reliable utility service and infrastructure at reasonable rates, with a commitment to environmental enhancement and a healthy California economy"…

Policy: The Utility has a published Privacy Policy covering the EV recharging/billing application

Customer: The Customer's selected settings for policy options presented via customer-facing interfaces.

## 2.2 Applicable Privacy Policies

### Task #3: Privacy Policy Conformance Criteria

**Objective** Define and describe the criteria for conformance of a system or business process (identified in the use case and inventory) with an applicable privacy policy. As with the Use Case Inventory described in Task #2 above, the conformance criteria should align with the equivalent elements in the Detailed Privacy Use Case Analysis described in Section 3. Wherever possible, they should be grouped by the relevant FIP/Ps and expressed as privacy constraints.

Note that whereas Task #2 itemizes the environmental elements relevant to the Use Case, Task #3 focuses on the privacy requirements specifically.

**Example**

Privacy Policy Conformance Criteria:

(1) Ensure that the utility does not share data with third parties without the consumer's consent…etc.

(2) Ensure that the utility supports strong levels of:

(a) Identity authentication

(b) Security of transmission between the charging stations and the utility information systems…etc.

(3) Ensure that personal data is deleted on expiration of retention periods…

…

## 2.3 Initial Privacy Impact (or other) Assessment(s) [optional]

### Task #4: Assessment Preparation

**Objective** Prepare an initial privacy impact assessment, or as appropriate, a risk assessment, privacy maturity assessment, compliance review, or accountability model assessment applicable within the scope of analysis carried out in sections 2.1 and 2.2 above. Such an assessment can be deferred until a later iteration step (see Section 4.3) or inherited from a previous exercise.

**Example**

Since the Electric Vehicle (EV) has a unique ID, it can be linked to a specific customer. As such, customer's whereabouts may be tracked through utility transaction visibility…

The EV charging and vehicle management system may retain data, which can be used to identify patterns of charging and location information that can constitute PI.

Unless safeguards are in place and (where appropriate) under the customer control, there is a danger that intentionally anonymized PI nonetheless become PII…

The utility wishes to capture behavioral and movement patterns and sell this information to potential advertisers or other information brokers to generate additional revenue. This information constitutes PII. The collection and use of this information should only be done with the explicit, informed consent of the customer.

# 3 Develop Detailed Privacy Analysis

**Goal** Prepare and document a detailed Privacy Management Analysis of the Use Case which corresponds with the High Level Privacy Analysis and the High Level Use Case Description.

**Constraint** The Detailed Use Case must be clearly bounded and must include the following components.

## 3.1 Identify Participants and Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows

### Task #5: Identify Participants

**Objective** Identify Participants having operational privacy responsibilities.

**Definition** A "Participant" is any Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System within a Privacy Domain.

**Example**

*Participants Located at the Customer Site:*

Registered Customer

*Participants Located at the EV's Location:*

Registered Customer Host (Temporary host for EV charging), Registered Customer Guest

*Participants Located within the Utility's domain:*

Service Provider (Utility)

Contractors and Suppliers to the Utility

### Task #6: Identify Systems

**Objective** Identify the Systems where PI is collected, communicated, processed, stored or disposed within a Privacy Domain.

**Definition** For purposes of this specification, a System is a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management.

**Example**

*System Located at the Customer Site(s):*

Customer Communication Portal

EV Physical Re-Charging and Metering System

*System Located in the EV(s):*

EV: Device

EV On-Board System: System

*System Located within the EV manufacturer's domain:*

EV Charging Data Storage and Analysis System

*System Located within the Utility's domain:*

EV Program Information System (includes Rates, Customer Charge Orders, Customers enrolled in the program, Usage Info etc.)

EV Load Scheduler System

Utility Billing System

Remote Charge Monitoring System

Partner marketing system for transferring usage pattern and location information

### Task #7: Identify Privacy Domains and Owners

| | |
|---|---|
| **Objective** | Identify the Privacy Domains included in the use case together with the respective Domain Owners. |
| **Definition** | A "Domain" covers both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner. |
| | A "Domain Owner" is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain. |
| **Context** | Privacy Domains may be under the control of data subjects or Participants with a specific responsibility within a Privacy Domain, such as data controllers; capability providers; data processors; and other distinct entities having defined operational privacy management responsibilities. |
| **Rationale** | Domain Owner identification is important for purposes of establishing accountability. |

**Example**

*Utility Domain:*

The physical premises located at…. which includes the Utility's program information system, load scheduling system, billing system, and remote monitoring system

This physical location is part of a larger logical privacy domain, owned by the Utility and extends to the Customer Portal Communication system at the Customer's site, and the EV On-Board software application System installed in the EV by the Utility, together with cloud-based services hosted by….

*Customer Domain:*

The physical extent of the customer's home and adjacent land as well as the EV, wherever located, together with the logical area covered by devices under the ownership and control of the customer (such as mobile devices).

**Example**

The EV On-Board System belongs to the utility Privacy Domain Owner.

The EV (with its ID Number) belongs to the Customer Domain Owner and the Vehicle Manufacturer Domain Owners, but the EV ID may be accessed by the Utility.

### Task #8: Identify Roles and Responsibilities within a Domain

**Objective** For any given use case, identify the roles and responsibilities assigned to specific Participants and Systems within a specific privacy domain

**Rationale** Any Participant may carry multiple roles and responsibilities and these need to be distinguishable, particularly as many functions involved in processing of PI are assigned to functional roles, with explicit authority to act, rather to specific participant.

**Example**

| | |
|---|---|
| Role: | EV Manufacturer Privacy Officer |
| Responsibilities: | Ensure that all PI data flows from EV On-Board System conform with contractual obligations associated with the Utility and vehicle owner as well as the Collection Limitation and Information Minimization FIP/P. in its privacy policies. |

### Task #9: Identify Touch Points

**Objective** Identify the touch points at which the data flows intersect with Privacy Domains or Systems within Privacy Domains.

**Definition** Touch Points are the intersections of data flows with Privacy Domains or Systems within Privacy Domains.

**Rationale** The main purpose for identifying touch points in the use case is to clarify the data flows and ensure a complete picture of all Privacy Domains and Systems in which PI is used.

**Example**

The Customer Communication Portal provides an interface through which the Customer communicates a charge order to the Utility. This interface is a touch point.

When the customer plugs into the charging station, the EV On-Board System embeds communication functionality to send EV ID and EV Charge Requirements to the Customer Communication Portal. This functionality provides a further touch point.

### Task #10: Identify Data Flows

**Objective** Identify the data flows carrying PI and privacy constraints among Domains in the Use Case.

**Constraint** Data flows may be multidirectional or unidirectional.

**Example**

When a charging request event occurs, the Customer Communication Portal sends Customer information, EV identification, and Customer Communication Portal location information to the EV Program Information System managed by the Utility.

This application uses metadata tags to indicate whether or not customer' identification and location data may be shared with authorized third parties, and to prohibit the sharing of data that provides customers' movement history, if derived from an aggregation of transactions.

## 3.2 Identify PI in Use Case Privacy Domains and Systems

**Objective** Specify the PI collected, created, communicated, processed or stored within Privacy Domains or Systems in three categories.

### Task #11: Identify Incoming PI

**Definition** Incoming PI is PI flowing into a Privacy Domain, or a system within a Privacy Domain.

**Constraint** Incoming PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

### Task #12: Identify Internally Generated PI

**Definition** Internally Generated PI is PI created within the Privacy Domain or System itself.

**Constraint** Internally Generated PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

**Example** Examples include device information, time-stamps, location information, and other system-generated data that may be linked to an identity.

### Task #13: Identify Outgoing PI

**Definition** Outgoing PI is PI flowing out of one system to another system within a Privacy Doman or to another Privacy Domain.

**Constraint** Outgoing PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

**Example**

*Incoming PI:*

Customer ID received by Customer Communications Portal

*Internally Generated PI:*

Current EV location associated with customer information, and time/location information logged by EV On-Board system

*Outgoing PI:*

Current EV ID and location information transmitted to Utility Load Scheduler System

## 3.3 Specify Required Privacy Controls Associated with PI

**Goal** For Incoming, Internally Generated and Outgoing PI, specify the privacy controls required to enforce the privacy policy associated with the PI. Privacy controls may be pre-defined or may be derived. In either case, privacy controls are typically associated with specific Fair Information Practices Principles (FIP/Ps) that apply to the PI.

**Definition** Control is a process designed to provide reasonable assurance regarding the achievement of stated objectives.

**Definition** Privacy Controls are administrative, technical and physical safeguards employed within an organization or Privacy Domain in order to protect PI. They are the means by which privacy policies are satisfied in an operational setting.

### Task #14: Specify Inherited Privacy Controls

**Objective** Specify the required Privacy Controls which are inherited from Privacy Domains or Systems within Privacy Domains.

**Example:**

The utility inherits a Privacy Control associated with the Electric Vehicle's ID (EVID) from the vehicle manufacturer's privacy policies.

The utility inherits the consumer's Operational Privacy Control Requirements, expressed as privacy preferences, via a link with the customer communications portal when she plugs her EV into friend Rick's charging station.

The utility must apply Jane's privacy preferences to the current transaction. The Utility accesses Jane's privacy preferences and learns that Jane does not want her association with Rick exported to the Utility's third party partners. Even though Rick's privacy settings differ around his PI, Jane's non-consent to the association being transmitted out of the Utility's privacy domain is sufficient to prevent commutative association. Thus if Rick were to charge his car's batteries at Jane's, the association between them would also not be shared with third parties.

### Task #15: Specify Internal Privacy Controls

**Objective** Specify the Privacy Controls which are mandated by internal Privacy Domain policies.

**Example**

**Use Limitation Internal Privacy Controls**

The Utility complies with California Code SB 1476 of 2010 (Public Utilities Code §§ 8380-8381 Use Limitation).

It implements the 2011 California Public Utility Commission (CPUC) privacy rules, recognizing the CPUC's regulatory privacy jurisdiction over it and third parties with which it shares customer data.

Further, it adopts NIST 800-53 Appendix J's "Control Family" on Use Limitation – e.g. it evaluates any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

### Task #16: Specify Exported Privacy Controls

**Objective** Specify the Privacy Controls which must be exported to other Privacy Domains or to Systems within Privacy Domains.

**Example**

The Utility exports Jane's privacy preferences associated with her PI to its third party partner, whose systems are capable of understanding and enforcing these preferences. One of her privacy control requirements is to not share her EVID with marketing aggregators or advertisers.

# 4 Identify Functional Services Necessary to Support Privacy Controls

Privacy controls are usually stated in the form of a policy declaration or requirement and not in a way that is immediately actionable or implementable. Until now, we have been concerned with the real-world, human side of privacy but we need now to turn attention to the digital world and "system-level" concerns. "Services" provide the bridge between those requirements and a privacy management implementation by providing privacy constraints on system-level actions governing the flow of PI between touch points.

## 4.1 Services Needed to Implement the Controls

A set of operational Services is the organizing structure which will be used to link the required Privacy Controls specified in Section 4.3 to operational mechanisms necessary to implement those requirements.

Eight Privacy Services have been identified, based on the mandate to support an arbitrary set of privacy policies, but at a *functional level*. The eight Services can be logically grouped into three categories:

- **Core Policy**: Agreement, Usage
- **Privacy Assurance**: Security, Validation, Certification, Enforcement
- **Presentation and Lifecycle**: Interaction, Access

These groupings, illustrated below, are meant to clarify the "architectural" relationship of the Services in an operational design. However, the functions provided by all Services are available for mutual interaction without restriction.

| ***Core Policy Services*** | ***Privacy Assurance Services*** | | ***Presentation & Lifecycle Services*** |
|---|---|---|---|
| Agreement | Validation | Certification | Interaction |
| Usage | Security | Enforcement | Access |

A system architect or technical manager should be able to integrate these privacy Services into a functional architecture, with specific mechanisms selected to implement these functions. In fact, a key purpose of the PMRM is to stimulate design and analysis of the specific functions - both manual and automated - that are needed to implement any set of privacy policies. In that sense, the PMRM is an analytic tool.

The PMRM identifies various system capabilities that are not typically described in privacy practices and principles. For example, a policy management (or "usage and control") function is essential to manage the PI usage constraints established by a data subject information processor or by regulation, but such a function is not explicitly named in privacy principles/practices. Likewise, interfaces (and agents) are not explicit in the privacy principles/practices, but are necessary to represent other essential operational capabilities.

Such inferred capabilities are necessary if information systems are to be made "privacy configurable and compliant." Without them, enforcing privacy policies in a distributed, fully automated environment will not be possible, and businesses, data subjects, and regulators will be burdened with inefficient and error-prone manual processing, inadequate privacy governance and compliance controls, and inadequate compliance reporting.

As used here,

- A "Service" is defined as a collection of related functions and mechanisms that operate for a specified purpose;
- An "Actor" is defined as a system-level, digital 'proxy' for either a (human) Participant or an (non-human) system-level process or other agent.

The eight privacy Services defined are **Agreement, Usage, Security, Validation, Certification, Enforcement, Interaction,** and **Access.** Specific operational behavior of these Services is governed by the privacy policy and constraints that are configured in a particular implementation and jurisdictional context. These will be identified as part of the Use Case analysis. Practice with use cases has shown that the Services listed above can, together, operationally encompass any arbitrary set of privacy requirements.

The functions of one Service may invoke another Service. In other words, functions under one Service may "call" those under another Service (for example, pass information to a new function for subsequent action). In line with principles of Service-Oriented Architecture (SOA)[2], the Services can thus interact in an arbitrary interconnected sequence to accomplish a privacy management task or set of privacy lifecycle requirements. Use cases will illustrate such interactions and their sequencing as the PMRM is used to solve a particular privacy problem. By examining and by solving multiple use cases, the PMRM can be tested for applicability and robustness.

The table below provides a description of each Service's functionality and an informal definition of each Service:

| SERVICE | FUNCTIONALITY | PURPOSE |
|---|---|---|
| **AGREEMENT** | Define and document permissions and rules for the handling of PI based on applicable policies, data subject preferences, and other relevant factors; provide relevant Actors with a mechanism to negotiate or establish new permissions and rules; express the agreements for use by other Services | Manage and negotiate permissions and rules |
| **USAGE** | Ensure that the use of PI complies with the terms of any applicable permission, policy, law or regulation,<br>including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization over the lifecycle of the use case | Control PI use |
| **VALIDATION** | Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors | Check PI |
| **CERTIFICATION** | Ensure that the credentials of any Actor, Domain, System , or system component are compatible with their assigned roles in processing PI; and verify their compliance and trustworthiness against defined policies and assigned roles. | Check credentials |
| **ENFORCEMENT** | Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate that an Actor or System does not conform to defined policies or the terms of a permission (agreement) | Monitor and respond to audited exception conditions |
| **SECURITY** | Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of personal information; make possible the trustworthy processing, communication, storage and disposition of privacy operations | Safeguard privacy information and operations |
| **INTERACTION** | Provide generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI; encompasses functionality such as user interfaces, system-to-system information exchanges, and agents | Information presentation and communication |
| **ACCESS** | Enable data-subjects , as required and/or allowed by permission, policy, or regulation, to review their PI that is held within a Domain and propose changes and/or corrections to their PI | View and propose changes to stored PI |

[2] See for example the **[SOA-RM]** and the **[SOA-RAF]**

| | | |
|---|---|---|

## 4.2 Service Details and Function Descriptions

### 4.2.1 Core Policy Services

#### 1. Agreement Service

- Define and document permissions and rules for the handling of PI based on applicable policies, individual preferences, and other relevant factors.
- Provide relevant Actors with a mechanism to negotiate or establish new permissions and rules.
- Express the agreements for use by other Services.

**Example**

As part of its standard customer service agreement, a bank requests selected customer PI, with associated permissions for use. Customer negotiates with the bank (whether via an electronic interface, by telephone or in person) to modify the permissions. Customer provides the PI to the bank, with the modified and agreed to permissions. This agreement is signed by both parties, stored in an appropriate representation and the customer is provided a copy.

#### 2. Usage Service

- Ensure that the use of PI complies with the terms of any applicable permission, policy, law or regulation,
- Including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization,
- Over the lifecycle of the use case.

**Example**

A third party has acquired specific PI, consistent with agreed permissions for use. Before using the PI, the third party has implemented functionality ensuring that the usage of the PI is consistent with these permissions.

### 4.2.2 Privacy Assurance Services

#### 3. Validation Service

- Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors.

**Example**

PI is received from an authorized third party for a particular purpose. Specific characteristics of the PI, such as date the information was originally provided, are checked to ensure the PI meets specified use requirements.

#### 4. Certification Service

- Ensure that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI;
- Verify that an Actor, Domain, System, or system component supports defined policies and conforms with assigned roles.

**Example**

A patient enters an emergency room, presenting identifying credentials. Functionality has been implemented which enables hospital personnel to check those credentials against a patient database information exchange. Additionally, the certification service's authentication processes ensures that the information exchange is authorized to receive the request.

#### 5. Enforcement Service

- Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate that an Actor or System does not conform to defined laws, regulations, policies or the terms of a permission (agreement).

**Example**

A magazine's subscription service provider forwards customer PI to a third party not authorized to receive the information. A routine audit of the service provider's system reveals this unauthorized disclosure practice, alerting the appropriate responsible official (the organization's privacy officer), who takes appropriate action.

#### 6. Security Service

- Make possible the trustworthy processing, communication, storage and disposition of privacy operations;
- Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of personal information.

**Example**

PI is transferred between authorized recipients, using transmission encryption, to ensure confidentiality.

Strong standards-based, identity, authentication and authorization management systems are implemented to conform to data security policies.

### 4.2.3 Presentation and Lifecycle Services

#### 7. Interaction Service

- Provide generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI;
- Encompasses functionality such as user interfaces, system-to-system information exchanges, and agents.

**Example:**

Your home banking application uses a graphical user interface (GUI) to communicate with you, including presenting any relevant privacy notices, enabling access to PI disclosures, and providing customer with options to modify privacy preferences.

The banking application utilizes email alerts to notify customers when policies have changed and uses postal mail to confirm customer-requested changes.

#### 8. Access Service

- Enable data-subjects, as required and/or allowed by permission, policy, or regulation, to review their PI held within a Domain and propose changes and/or corrections to it.

**Example:**

A national credit bureau has implemented an online service enabling customers to request their credit score details and to report discrepancies in their credit histories.

## 4.3 Identify Services satisfying the privacy controls

The Services defined in Section 4.1 encompass detailed Functions and Mechanisms needed to transform the privacy controls of section 3.3 into an operational system design for the use case. Since the detailed use case analysis focused on the data flows – incoming, internally generated, outgoing – between Systems (and Actors), the Service selections should be on the same granular basis.

### Task #17: Identify the Services necessary to support operation of identified privacy controls.

Perform this task for each data flow exchange of PI between systems.

This detailed conversion into Service operations can then be synthesized into consolidated sets of Service actions per System involved in the Use Case.

On further iteration and refinement, the engaged Services can be further delineated by the appropriate Functions and Mechanisms for the relevant privacy controls.

**Examples:**

Based upon

**a) Internally Generated PI** (Current EV location logged by EV On-Board system), and
**b) Outgoing PI** (Current EV location transmitted to Utility Load Scheduler System),
convert to operational Services as follows:

**"Log EV location":**

| | |
|---|---|
| **Validation** | EV On-Board System checks that the reporting of a particular charging location has been opted-in by EV owner |
| **Enforcement** | If location has not been authorized by EV Owner for reporting and the location data has been transmitted, then notify the Owner and/or the Utility |
| **Interaction** | Communicate EV Location to EV On-Board System |
| **Usage** | EV On-Board System records EV Location in secure storage; EV location data is linked to agreements |

**"Transmit EV Location to Utility Load Scheduler System (ULSS)":**

| | |
|---|---|
| **Interaction** | Communication established between EV Location and ULSS |
| **Security** | Authenticate the ULSS site; secure the transmission |
| **Certification** | ULSS checks the credentials of the EV On-Board System |
| **Validation** | Validate the EV Location against accepted locations |
| **Usage** | ULSS records the EV Location, together with agreements |

# 5 Define the Technical Functionality and Business Processes Supporting the Selected Services

Each Service is composed of a set of operational Functions, reflected in defined business processes and technical solutions.

The **Functions** step is critical because it necessitates either designating the particular business process or technical mechanism being implemented to support the Services required in the use case or the absence of such a business process or technical mechanism.

## 5.1 Identify Functions Satisfying the Selected Services

Up to this point in the PMRM methodology, the primary focus of the use case analysis has been on the "what" - PI, policies, control requirements, the Services needed to manage privacy. Here the PMRM requires a statement of the "how" – what business processes and technical mechanisms are identified as providing expected functionality.

Task #18: **Identify the Functions that satisfy the selected Services**

**Examples**

**"Log EV Location"** (uses services **Validation**, **Enforcement**, **Interaction**, and **Usage** Services)**:**

**Function:** Encrypt the EV Location and Agreements and store in on-board solid-state drive

**"Transmit EV Location to Utility Load Scheduler System (ULSS)"** (uses **Interaction**, **Security**, **Certification**, **Validation**, and **Usage** Services):

**Function:** Establish a TLS/SSL communication between EV Location and ULSS, which includes mechanisms for authentication of the source/destination

# 6 Perform Risk and/or Compliance Assessment

## Task #19: Conduct Risk Assessment

**Objective** Once the requirements in the Use Case have been converted into operational Services, an overall risk assessment should be performed from that operational perspective

**Constraint** Additional controls may be necessary to mitigate risks within Services. The level of granularity is determined by the Use Case scope. Provide operational risk assessments for the selected Services within the use case.

**Examples**

**"Log EV location":**

| | |
|---|---|
| **Validation** | EV On-Board System checks that location is not previously rejected by EV owner<br>**Risk**: On-board System has been corrupted |
| **Enforcement** | If location is previously rejected, then notify the Owner and/or the Utility<br>**Risk**: On-board System not current |
| **Interaction** | Communicate EV Location to EV On-Board System<br>**Risk**: Communication link not available |
| **Usage** | EV On-Board System records EV Location in secure storage, together with agreements<br>**Risk**: Security controls for On-Board System are compromised |

**"Transmit EV Location to Utility Load Scheduler System (ULSS)":**

| | |
|---|---|
| **Interaction** | Communication established between EV Location and ULSS<br>**Risk**: Communication link down |
| **Security** | Authenticate the ULSS site; secure the transmission<br>**Risk**: ULSS site credentials are not current |
| **Certification** | ULSS checks the credentials of the EV On-Board System<br>**Risk**: EV On-Board System credentials do not check |
| **Validation** | Validate the EV Location against accepted locations<br>**Risk**: Accepted locations are back-level |
| **Usage** | ULSS records the EV Location, together with agreements<br>**Risk**: Security controls for the ULSS are compromised |

# 7 Initiate Iterative Process

**Goal** A 'first pass' through the Tasks above can be used to identify the scope of the Use Case and the underlying privacy policies and constraints. Additional iterative passes would serve to refine the Use Case and to add detail. Later passes could serve to resolve "TBD" sections that are important, but were not previously developed.

Note that a 'single pass' analysis might mislead the PMRM user into thinking the Use Case was fully developed and understood. Iterative passes through the analysis will almost certainly reveal further details. Keep in mind that the ultimate objective is to develop insight into the Use Case sufficient to provide a reference model for an operational, Service-based, solution.

## Task #20: **Iterate the analysis and refine.**

Iterate the analysis in the previous sections, seeking further refinement and detail.

# 8 Operational Definitions for Fair Information Practices/Principles ("FIPPs") and Glossary

As explained in the introduction, every specialized domain is likely to create and use a domain-specific vocabulary of concepts and terms that should be used and understood in the specific context of that domain. PMRM is no different and this section contains such terms.

In addition, a number of "operational definitions" are intended to be used in the PMRM to support development of the "Detailed Privacy Use Case Analysis" described in Section 4. Their use is completely optional, but may be helpful in organizing privacy policies and controls where there are inconsistencies in definitions across policy boundaries or where existing definitions do not adequately express the operational characteristics associated with Fair Information Practices/Principles.

## 8.1 Operational FIPPs

The following 14 Fair Information Practices/Principles are composite definitions derived from a comprehensive list of international legislative instruments. These operational FIPPs can serve as a sample set, as needed.

**Accountability**

Functionality enabling reporting by the business process and technical systems which implement privacy policies, to the data subject or Participant accountable for ensuring compliance with those policies, with optional linkages to redress and sanctions.

**Notice**

Functionality providing Information, in the context of a specified use, regarding policies and practices exercised within a Privacy Domain including: definition of the Personal Information collected; its use (purpose specification); its disclosure to parties within or external to the domain; practices associated with the maintenance and protection of the information; options available to the data subject regarding the processor's privacy practices; retention and deletion; changes made to policies or practices; and other information provided to the data subject at designated times and under designated circumstances.

**Consent**

Functionality, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, enabling data subjects to agree to the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

**Collection Limitation and Information Minimization**

Functionality, exercised by the information processor, that limits the information collected, processed, communicated and stored to the minimum necessary to achieve a stated purpose and, when required, demonstrably collected by fair and lawful means.

**Use Limitation**

Functionality, exercised by the information processor, that ensures that Personal Information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes.

**Disclosure**

Functionality that enables the transfer, provision of access to, use for new purposes, or release in any manner, of Personal Information managed within a Privacy Domain in accordance with notice and consent permissions and/or applicable laws and functionality making known the information processor's policies to external parties receiving the information.

**Access and Correction**

Functionality that allows an adequately identified data subject to discover, correct or delete, Personal Information managed within a Privacy Domain; functionality providing notice of denial of access; and options for challenging denial when specified.

**Security/Safeguards**

Functionality that ensures the confidentiality, availability and integrity of Personal Information collected, used, communicated, maintained, and stored; and that ensures specified Personal Information will be de-identified and/or destroyed as required.

**Information Quality**

Functionality that ensures that information collected and used is adequate for purpose, relevant for purpose, accurate at time of use, and, where specified, kept up to date, corrected or destroyed.

**Enforcement**

Functionality that ensures compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

**Openness**

Functionality, available to data subjects, that allows access to an information processors policies and practices relating to the management of their Personal Information and that establishes the existence, nature, and purpose of use of Personal Information held about the data subject.

**Anonymity**

Functionality that prevents data being collected or used in a manner that can identify a specific natural person.

**Information Flow**

Functionality that enables the communication of personal information across geo-political jurisdictions by private or public entities involved in governmental, economic, social or other activities.

**Sensitivity**

Functionality that provides special handling, processing, security treatment or other treatment of specified information, as defined by law, regulation or policy.

## 8.2 Glossary

**Actor**

A system-level, digital 'proxy' for either a (human) Participant (or their delegate) interacting with a system or a (non-human) in-system process or other agent.

**Audit Controls**

Processes designed to provide reasonable assurance regarding the effectiveness and efficiency of operations and compliance with applicable policies, laws, and regulations.

**Boundary Object**

A sociological construct that supports productive interaction and collaboration among multiple communities.

**Control**

A process designed to provide reasonable assurance regarding the achievement of stated objectives.

**Domain Owner**

A Participant having responsibility for ensuring that privacy controls and privacy constraints are implemented and managed in business processes and technical systems in accordance with policy and requirements.

**Incoming PI**

PI flowing into a Privacy Domain, or a system within a Privacy Domain.

**Internally Generated PI**

PI created within the Privacy Domain or System itself.

**Monitor**

To observe the operation of processes and to indicate when exception conditions occur.

**Outgoing PI**

PI flowing out of one system to another system within a Privacy Doman or to another Privacy Domain.

**Participant**

A Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System within a Privacy Domain.

**PI**

Personal Information – any data which describes some attribute of, or that is uniquely associated with, a natural person.

**PII**

Personally identifiable information – any (set of) data that can be used to uniquely identify a natural person.

**Policy**

Laws, regulations, contractual terms and conditions, or operational rules or guidance associated with the collection, use, transmission, storage or destruction of personal information or personally identifiable information

**Privacy Architecture**

A collection of proposed policies and practices appropriate for a given domain resulting from use of the PMRM

**Privacy Constraint**

An operational mechanism that controls the extent to which PII may flow between touch points.

**Privacy Control**

An administrative, technical or physical safeguard employed within an organization or Privacy Domain in order to protect PII.

**Privacy Domain**

A physical or logical area within the use case that is subject to the control of a Domain Owner(s)

**Privacy Management**

The collection of policies, processes and methods used to protect and manage PI.

**Privacy Management Analysis**

Documentation resulting from use of the PMRM and that serves multiple Stakeholders, including privacy officers and managers, general compliance managers, and system developers

**Privacy Management Reference Model and Methodology (PMRM)**

A model and methodology for understanding and analyzing privacy policies and their management requirements in defined use cases; and for selecting the technical services which must be implemented to support privacy controls.

**(PMRM) Service**

A collection of related functions and mechanisms that operate for a specified purpose.

**System**

A collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management.

**Touch Point**

The intersection of data flows with Privacy Domains or Systems within Privacy Domains.

# Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

**Participants:**

Peter F Brown, Individual Member
Gershon Janssen, Individual Member
Dawn Jutla, Saint Mary's University
Gail Magnuson, Individual Member
Joanne McNabb, California Office of Privacy Protection
John Sabo, Individual Member
Stuart Shapiro, MITRE Corporation
Michael Willett, Individual Member

# Appendix B. Revision History

| Revision | Date | Editor | Changes Made |
|---|---|---|---|
| WD05 | 2012-10-17 | John Sabo | Incorporate agreed dispositions to issues raised during First Public Review |
| WD05 | 2012-10-19 | Peter F Brown | Minor edits, terminology alignment and clean-up of formatting |
| WD05 | 2012-10-31 | Peter F Brown | This document |