The Privacy Management Reference Model (PMRM) and Methodology

Dawn N. Jutla, PhD

Member, OASIS PMRM Technical Committee

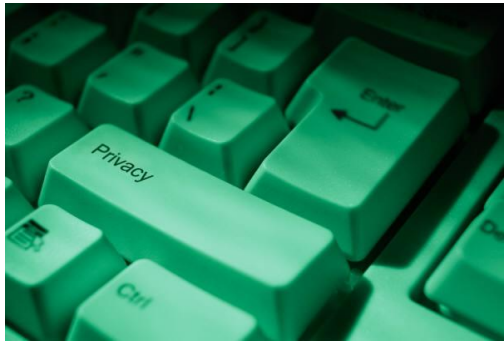
Author, Layering Privacy on Operating Systems, Social Networks, and other Platforms by Design

Professor, Sobey School of Business, Saint Mary's University, Halifax, Nova Scotia, Canada

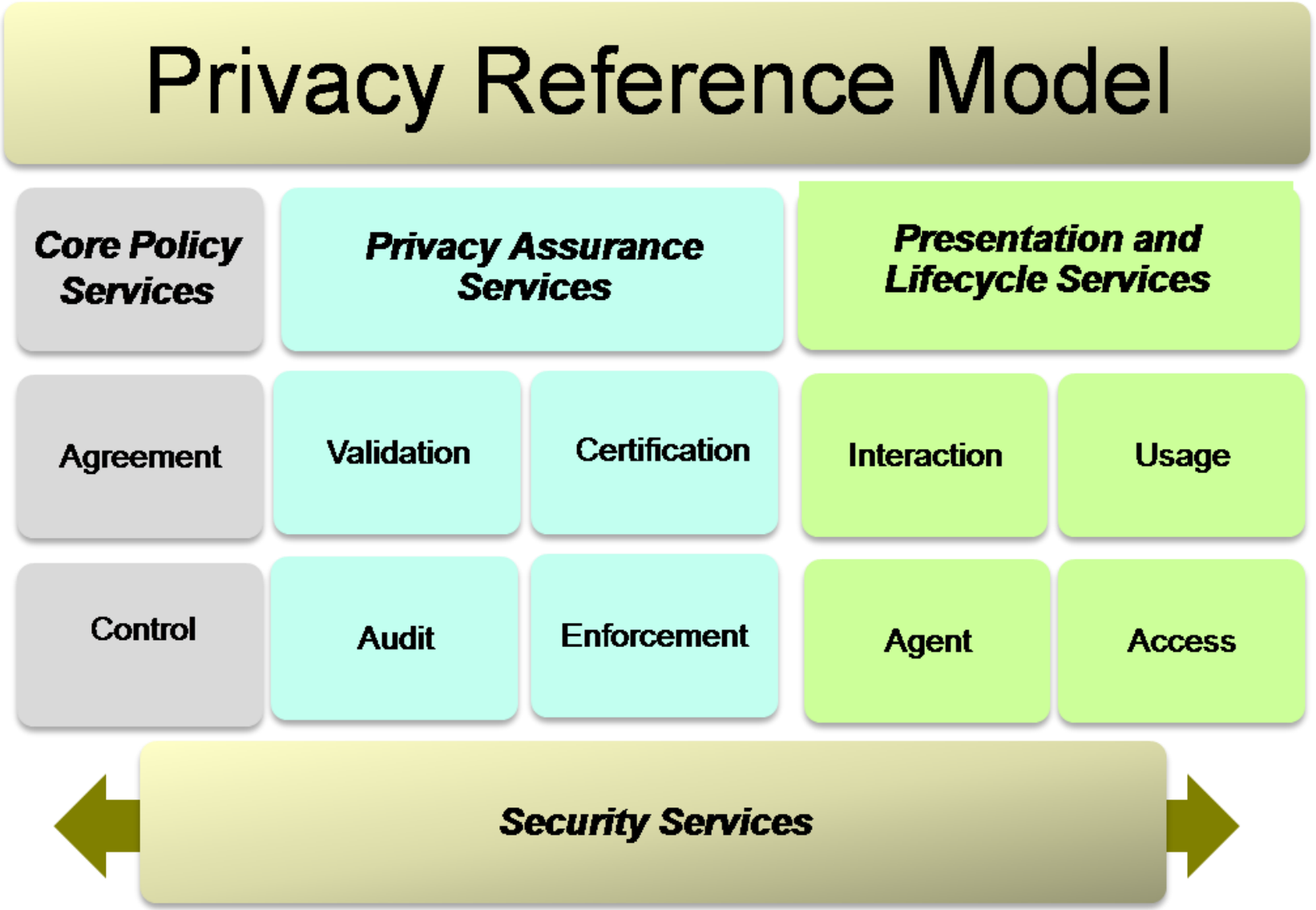
dawn.jutla@gmail.com OR dawn.jutla@smu.ca

Complex Privacy Landscape

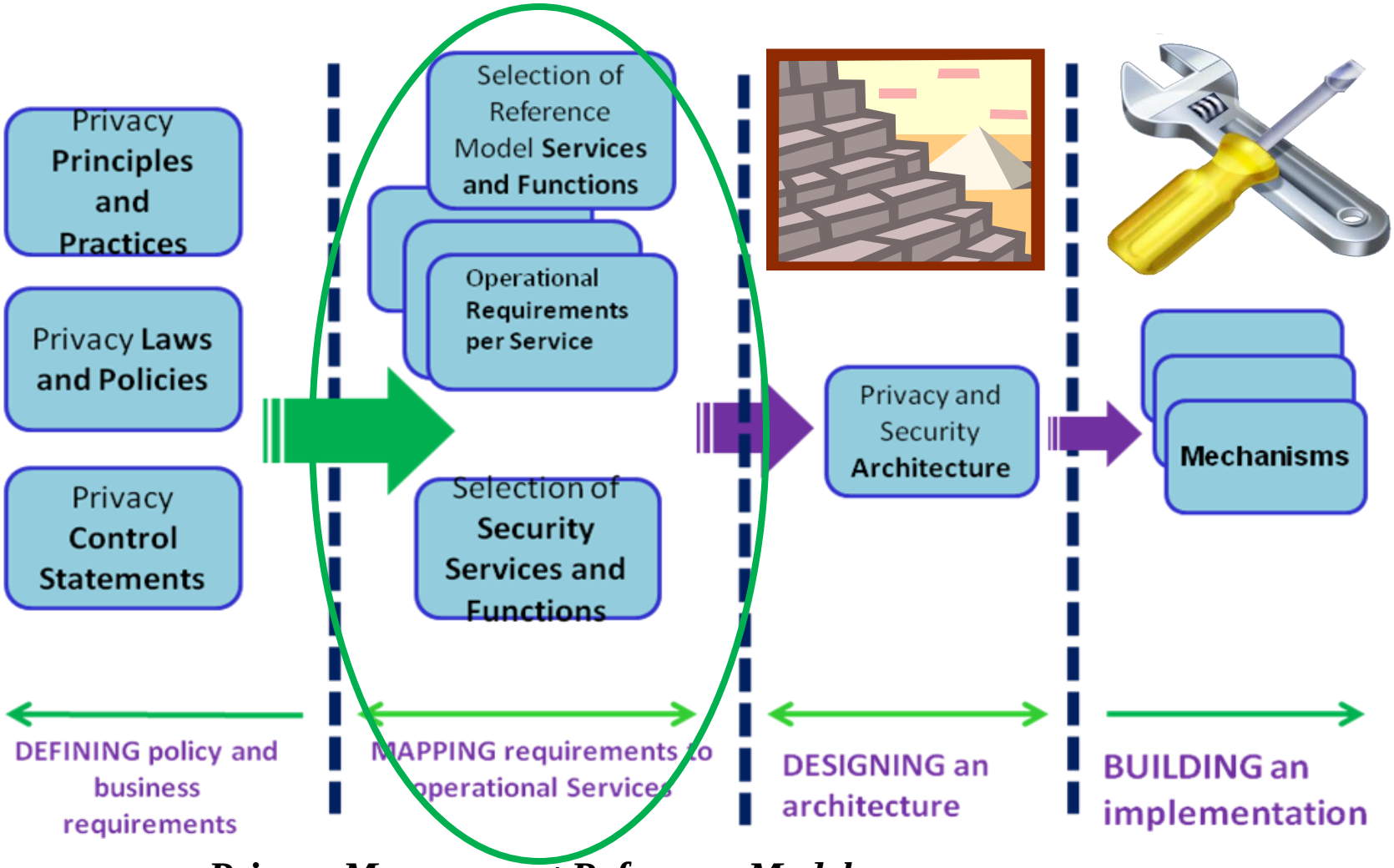
- The Privacy Act of 1974 (U.S.)
- Council of Europe Convention 108
- OECD Privacy Guidelines
- UN Guidelines Concerning Personalized Computer Files
- Hong Kong Personal Data (Privacy) Ordinance
- EU Data Protection Directive 95/46/EC
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
- International Labour Organization (ILO) Code of Practice on the Protection of Workers' Personal Data
- US FTC statement of Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Ontario Privacy Diagnostic Tool
- Australian Privacy Act – National Privacy Principles
- California Senate Bill 1386, "Security Breach Notification"
- AICPA/CICA Privacy Framework
- Japan Personal Information Protection Act
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework



Fair Information Practice Principles are mapped to each PMRM Service



Where Does the Reference Model Fit?



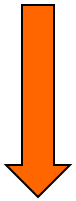
Privacy Management Reference Model

PMRM Validation Service

The Validation Service evaluates and, as required, ensures information minimization and quality in terms of accuracy, completeness, relevance and timeliness of PI at particular points in the information lifecycle.

Addresses: Information minimization, Collection limitation, Information Quality, Pseudonymity, Anonymity (in part).

Specific
e.g. Birthdate/Salary/IQ



General
e.g. Age range – over 50, salary range, or IQ range

Access Control
e.g Role-based, User-directed

...

Cryptography

View Mechanisms

Fragmentation Mechanisms

PMRM Methodology

Step-by-step Instructions and Guidance

1

DEFINE SCOPE OF PMRM and APPLICATION IMPACTING PERSONALLY IDENTIFIABLE INFORMATION

1.0 Determine scope of PMRM Analysis

Guidance e.g. (a) To conduct the general Privacy Impact Assessment, AND/OR
(b) To conduct an Accountability Review, AND/OR
(c) To identify what privacy services are required at PI or PII touch points in information systems.

1.1 Define the particular business system, process(es), product(s), environment, service(s), system(s), data, and/or application(s) which will impact the collection, communication, processing, storage or destruction of PI or PII

1.2 Define use case scenarios

2

CONDUCT INITIAL REVIEW OF THE USE CASES

2.1 Assess the need and efficacy of using PI throughout the defined Use Cases

2.2 Determine the FIPPs and/or applicable privacy and data protection framework applicable to eachUse Case

Examples: (Country: USA) HIPAA security and privacy requirements
(State: California) Health Information Privacy – See http://www.privacyprotection.ca.gov/privacy_laws.htm#four
(City: Sacramento) City of Sacramento Emergency Response Center Privacy Policy

2.3 Create and a set of draft assumptions, issues and recommendations to guide the detailed PMRM assessment stage

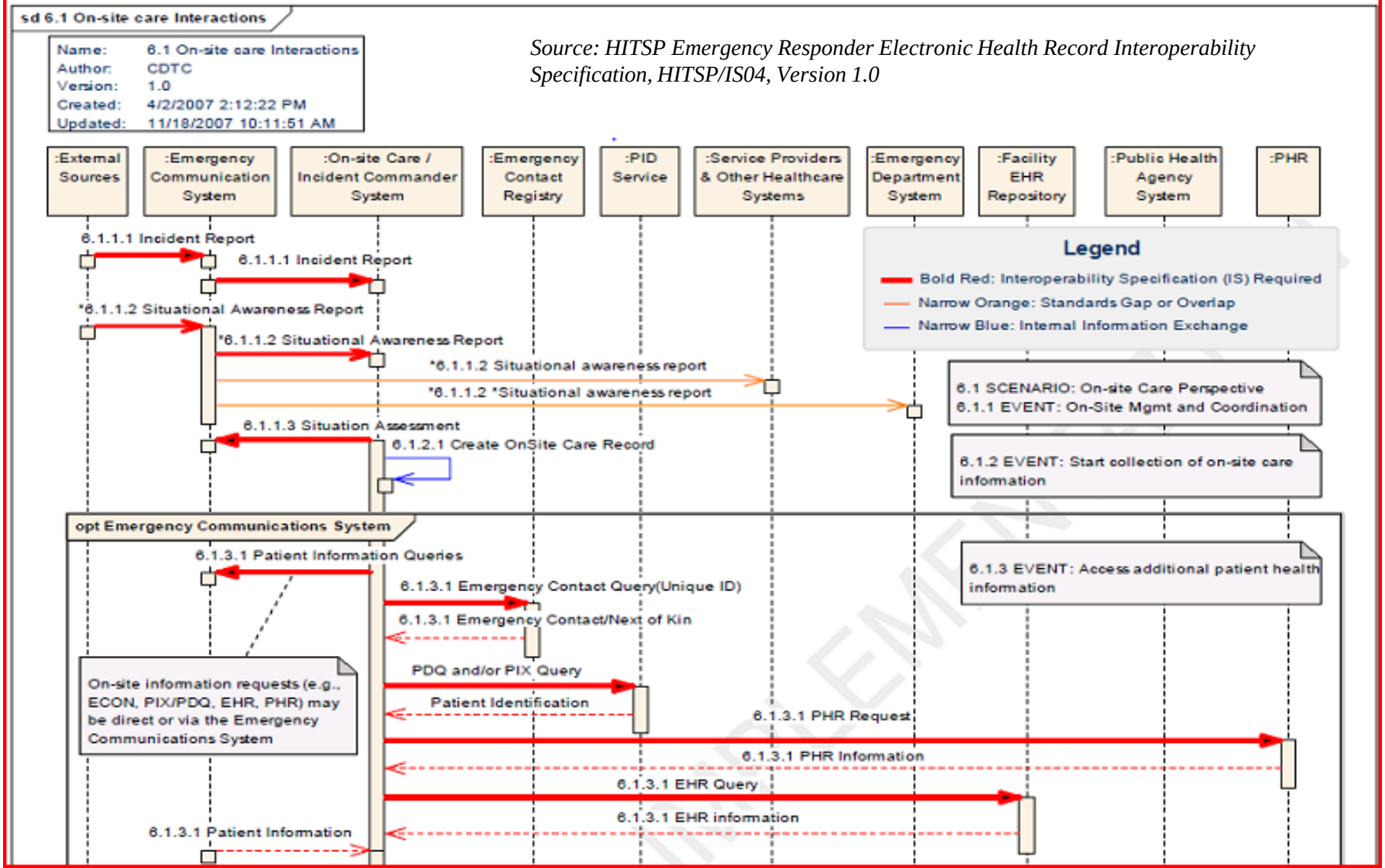
2.3.1 Establish whether (a) each regulation's requirements is applicable across all actors in each use case, and/or (b) any special or unique requirements/ rules associated with particular actors or touch points (e.g., communicating PHI in unencrypted communications or separation of patient payment and health information at point of treatment), and/or (c) cross-jurisdictional and technical contexts for interoperability are required.

Guidance e.g. : In the HITSP ER EHR use case on-site care scenario, examples of a) are the Personal Health Record provider actors which generally are not under HIPAA requirements in the USA, Examples of b) depend on regulations, organizational privacy policy, and business model. An example of c) is provided below in section 3.1.3 which discusses context.

3 **Describe the business processes and data flows using a data lifecycle description model and provide the level of detail needed to include <u>all actors and touch points</u>**

Figure 2.2.4.1-1 On-Site Care Scenario Perspective Business Sequence Diagram

Source: HITSP Emergency Responder Electronic Health Record Interoperability Specification, HITSP/IS04, Version 1.0



4 **4.1 For each actor instance, and incoming/outcoming data flow within a use case instance, (a) add context to requirements, and (b) determine the PMRM Services**

Table 1. Data Flows TO a Single Actor with PMRM Service Invocations.

ACTOR: ECS	PI-In Incoming Data Flows	Actor Source	Requirements [Examples – Qualify with Context]	PMRM SVCs	[Context Narrative]	Comment
	Incident Report	External sources	• ECS Privacy and Security Policy • jurisdictional regulations • OnStar	• Security • Control • Audit • Interaction • Validation • Usage	Incident involving Californians with all health info within the City of Sacramento	Data elements require further definition
	Situational Awareness Report	External Sources	• ECS Privacy and Security Policy • jurisdictional regulations • OnStar	• Security • Control • Audit • Interaction • Validation • Usage		
	Patient EHR Information	Service Provider and other Healthcare systems	• HIPAA security and privacy rules • HITECH • 3rd party inherited policy agreements	• Security • Control • Audit • Interaction • Validation • Certification • Usage		If Individual access or enforcement are necessary to the ECS, then Access and enforcement services required
	Situation Assessment	On-site Care/Incident Commander	• General scene information	• None		

Soliciting Use Cases

(and, if possible, Business Sequence Diagrams)

from multiple domains

Questions?

Dawn N. Jutla, PhD, Member, OASIS PMRM TC

dawn.jutla@gmail.com

John Sabo, co-Chair, OASIS PMRM TC

john.t.sabo@ca.com

Michael Willett, co-Chair, OASIS PMRM TC

mwillett@nc.rr.com

Dee Schur (OASIS)

dee.schur@oasis-open.org