Evolving OASIS Privacy by Design Standards

Dawn N. Jutla , PhD, Director, Board of OASIS
Professor of Computer Science and Business, Sobey School of Business, Saint Mary's University
Convener and co-Chair/co-editor, OASIS PbD-SE TC with Commissioner Ann Cavoukian; co-editor, OASIS PMRM

PRIVACY ENGINEERING WORKSHOP
April 9-10, 2014
National Institute of Standards and Technologies, US Dept. of Commerce

SAINT MARY'S UNIVERSITY
SOBEY
SCHOOL OF BUSINESS

EMERGING Standards to make **Privacy-by-Design** **Instinctual** on the **Internet**

FOR EVERY ORGANIZATION AND SOFTWARE ENGINEER – ON PURPOSE, IN A MANAGED WAY

OASIS
Advancing open standards for the information society

GARTNER 2014 PREDICTS:
By 2017, 80% of consumers will
collect, track and barter
their personal data for cost savings, convenience and customization.

Why should business care …

about consumer privacy & empowerment over personal data?

- Loss of customers, customer loyalty, stock value, and brand reputation
- Increased legal costs, class action lawsuits
- Shareholder and board dissatisfaction

OASIS PbD-SE


OASIS
Advancing open standards for the information society
Other Languages ▪ Site Map ▪ Member Login
I want to: take a tour of OASIS
GO
Standards | Committees | Join | News | Events | Resources | Member Sections | Policies | About
OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC
Join This TC
TC Members Page
Send A Comment
Enabling privacy to be embedded into IT system design and architecture
Dawn Jutla, dawn.jutla@gmail.com, Chair
Ann Cavoukian, Commissioner.ipc@ipc.on.ca, Chair
Gershon Janssen, gershon@qroot.com, Secretary
Table of Contents
Announcements
Overview
Subcommittees
TC Liaisons
Technical Work Produced by the Committee
Expository Work Produced by the Committee
External Resources
Mailing Lists and Comments
Press and Commentary
Additional Information
Search
Connect with OASIS
Related links
Charter
IPR Statement
Membership
Obligated Members
Email Archives
Comments Archive
Ballots
Documents
Schedule
TC Sponsors
Microsoft
Nokia Corporation
SecureKey Technologies, Inc.
Veterans Health Administration
Organizations listed above are OASIS Sponsor-level members who have representatives serving on

OASIS PMRM

OASIS
Advancing open standards for the information society

Other Languages ▪ Site Map ▪ **Member Login**

I want to: take a tour of OASIS GO

Standards | Committees | Join | News | Events | Resources | Member Sections | Policies | About

OASIS Privacy Management Reference Model (PMRM) TC

Search

Connect with OASIS

Join This TC | TC Members Page | Send A Comment

Providing a guideline for developing operational solutions to privacy issues

Michael Willett, mwillett@nc.rr.com, Chair
John Sabo, john.annapolis@verizon.net, Chair
Gershon Janssen, gershon@qroot.com, Secretary

Table of Contents

Related links

Charter
IPR Statement
FAQ
Membership
Obligated Members
Email Archives
Comments Archive
Ballots
Documents
Schedule
Press

TC Sponsors

NIST
Primeton Technologies, Inc.
Veterans Health Administration

Organizations listed above are OASIS Sponsor-level members who have representatives serving on this TC.

Announcements

Participation in the OASIS PMRM TC is open to all interested parties, including privacy policy makers, privacy and security consultants, auditors, IT systems architects and designers of systems that collect, process, use, share, transport, secure, or destroy Personal Information. OASIS also invites representatives of other TCs, external organizations, and standards bodies that may find the PMRM useful in developing privacy management use cases in their contexts. Contact member-services@oasis-open.org for more information on joining the TC.

Overview

The OASIS PMRM TC works to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations. PMRM picks up where broad privacy policies

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

1. PbD principles are internationally recognized with mappings/ alignment to FIPPs, GAPPs and NIST 800-53 Appendix J controls.

2. Help stakeholders to **visualize** privacy requirements and design from software conception to retirement

3. A specification of a methodology, mappings, and guidance to help software engineers to :
   - Model and translate Privacy by Design (PbD) principles to conformance requirements within software engineering tasks,
   - Produce privacy-aware software, and document artifacts as evidence of PbD-principle compliance.
   - Collaborate with management and auditors to *simplify* demonstration of compliance/audits.

OASIS Privacy Management Reference Model and Methodology (PMRM) Emerging Standard

TC Chair: John T. Sabo, Retired TC co-Chair: Michael Willett

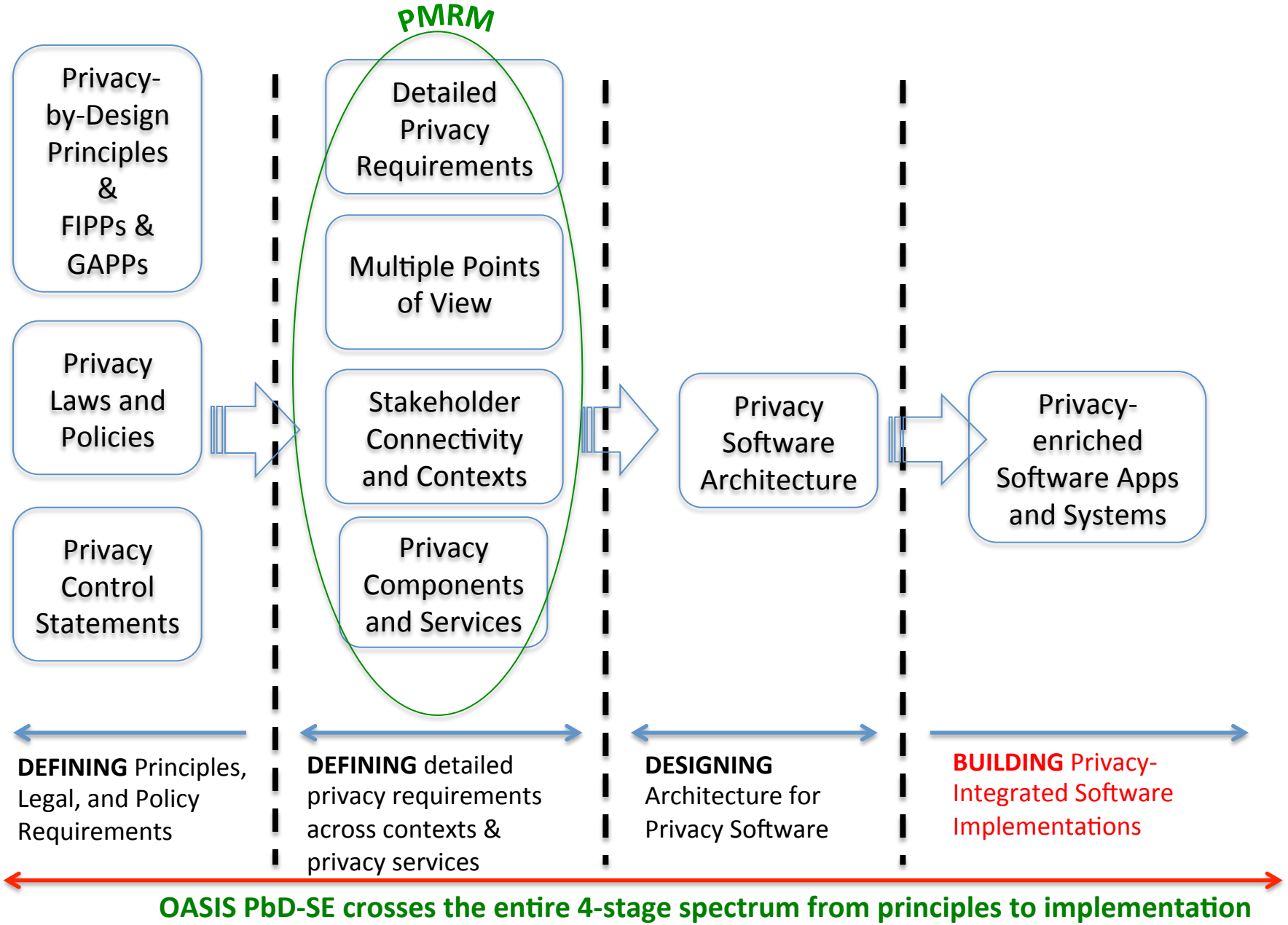
1. PMRM provides a model and methodology for translating & mapping privacy requirements,, as the basis for a PRIVACY SERVICE ARCHITECTURE: http://j.mp/oasisPMRM

2. KEY STRENGTH: Gets at how personal data flow among data platforms... 360 stakeholder view of privacy requirements.

3. Major elements of this emerging standard's methodology and the PbD-SE methodology unify and align with the state-of-the-art in the:
   - Dennedy, Finneran, and Fox's Privacy Engineering Manifesto book (industry-led – McAfee)
   - Shostack's Threat Modeling book (industry led- Microsoft)
   - Content in the Privacy Engineering program at Carnegie Mellon and extant privacy literature (university-led)

OASIS
Advancing open standards for the information society

Scope of the OASIS PbD-SE and OASIS PMRM Standard-Track Work Products



OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

Applicable to all organizations and individuals producing Information Technology Products and Services

Software Engineer: A person that adopts engineering approaches, such as established methodologies, processes, architectures, measurement tools, standards, organization methods, management methods, quality assurance systems and the like, in the development of large scale software, seeking to result in high productivity, low cost, controllable quality, and measurable development schedule.

Source: Adapted from Y. Wang, Senior Member of the IEEE and ACM. Theoretical Foundations of Software Engineering, Schulich School of Engineering, University of Calgary, 2011.

Large scale software extends to include apps that scale to millions of users

Organizations and individuals adopting design processes, privacy methodologies, models, and standards to obtain better user privacy going forward.

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

RACI Definitions

R – **Who is Responsible**
- The person who is assigned to do the work

A – **Who is Accountable**
- The person who makes the final decision and has the ultimate ownership

C – **Who is Consulted**
- The person who must be consulted before a decision or action is taken

I – **Who is Informed**
- The person who must be informed that a decision or action has been taken

RACI Chart for OASIS PbD-SE Methodology (WIP)

PbD-SE Methodology Step	Documented Activity	Software Engineer	Privacy Resource	Project Mgmt.	Mgmt.	Third Party	User
3.1 Assess Organization-al Readiness	Document Privacy Policy Document	C I	R A C I	C I	A C I	I	C I
	Document Privacy Roles/Training Program in Organization	I	R A C I	C I	A I	I	I
3.2 Scope Privacy Requirements & Reference Architecture	Document Functional Privacy Requirements & hooks to Reference Architecture	R A	R A C I	A C I	A I	R A I	C I
3.3 Conduct Risk Analysis on Use Cases	Document Business Model with Personal Data Flows	C I	R A C I	C I	A C	C I	-
	Document Risk analysis (incl. threat models, PIA)	C I	R A C I	C I	A C I	C I	-
3.4 Identify Privacy Resource Allocation	Document privacy resource allocation to SE team	I	R A C I	R I	A I	I	-
3.5 Create RACI for Producing Artifacts	Document RACI assignment to artifact production	R C I	C I	R A C I	A I	-	-
3.6 Customize Privacy Architecture	Document Privacy Architecture	R A	A C I	A C I	A I	I	-
3.7 Conduct Periodic Review	Document Review of Artifacts throughout the PDLC	R A	C I	R A C I	A I	-	-
3.8 Execute Code Testing & Privacy Evaluation	Document testing and evaluation for privacy usability - **metrics**	R A	R C I	R A C I	A I	-	C
3.9 Create Retirement Plan	Document plan for retirement of software solution	C I	R A C I	R A C I	A C I	I	I
3.10Sign-off	Document sign off with checklist	R A C I	R A C I	R A C I	A C	-	-

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

PbD "Sub-Principles"	*Compliance Criteria*	*Requirement(s)*
I. *Proactive* not Reactive; *Preventative* not Remedial		
I.1–Demonstrable Leadership: A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy protection, generally higher than prevailing legal requirements.	• Commitment to apply OASIS Specification to software engineering project	• Documentation MUST normatively reference PdD-se specification • Documentation MUST reference the applicable privacy policy
I.2–Defined Community of Practice: Demonstrable privacy commitment shared by organization members, user communities and stakeholders.	• Relevant stakeholders and team assembled for project	• Documentation must describe privacy champ, lead.. • Documentation MUST describe assignment of privacy resources to software teams, and responsibilities, accountability, consultation, and information supplied to all software stakeholders
I.3–Proactive and iterative: Continuous processes to identify privacy and data protection risks arising from poor designs, practices and outcomes, and to mitigate unintended or negative impacts in proactive and systematic ways.	• OASIS Specification applied throughout the software engineering life cycle. • Privacy metrics are defined and monitored in a system of regular reviews	• Project plan MUST include privacy section • Other documents SHOULD include privacy section *(might be limited to saying not applicable)* • Documentation MUST include privacy review reports *(either in reviewed documents or in separate report)* • Documentation MUST include defined privacy metrics.

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

PbD "Sub-Principles"	*Compliance Criteria*	*Requirement(s)*
2. Privacy as the *Default* Setting		
2.1–Purpose Specificity: Purposes must be specific and limited, and be amenable to engineering controls	• OASIS PbD-SE methodology and OASIS PMRM specifications applied For each functional use case/user story, document models of privacy requirements/design with the ***EQUIVALENT*** to the unified modeling language (UML) used in software engineering: Use Case Template or User Story Boards Use Case Diagram Misuse Case Diagram Class Diagram Activity Diagram Sequence Diagram	• The OASIS **PMRM** Privacy Use Case Template is RECOMMENDED for describing 360 ° view of stakeholder privacy requirements. • Documentation MUST describe functional use case /user story; privacy requirements; design requirements.
2.2–Adherence to Purposes: methods must be in place to ensure that personal data is collected, used and disclosed: • in conformity with specific, limited purposes; • in agreement with data subject consent; and • in compliance with applicable laws and regulations		
2.3–Engineering Controls: Strict limits should be placed on each phase of data processing lifecycle represented in software, including: • Limiting Collection; • Collecting by Fair and Lawful Means; • Collecting from Third Parties; • Uses and Disclosures; • Retention; • Disposal, Destruction; and Redaction • Transparency and Visibility	Document identification of privacy controls and services e.g. the PMRM-type Services: e.g. Agreement, Validation, Usage, Interaction, Certification, Security, Enforcement, and Access AND other e.g. Minimization, De-Identification, Monitoring, Data classification services.	• Documentation MUST describe data and behavioural requirements for each use case/user story, and possible misuses of data. • Documentation MUST describe selection of privacy controls/services and where they apply to functional requirements.

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

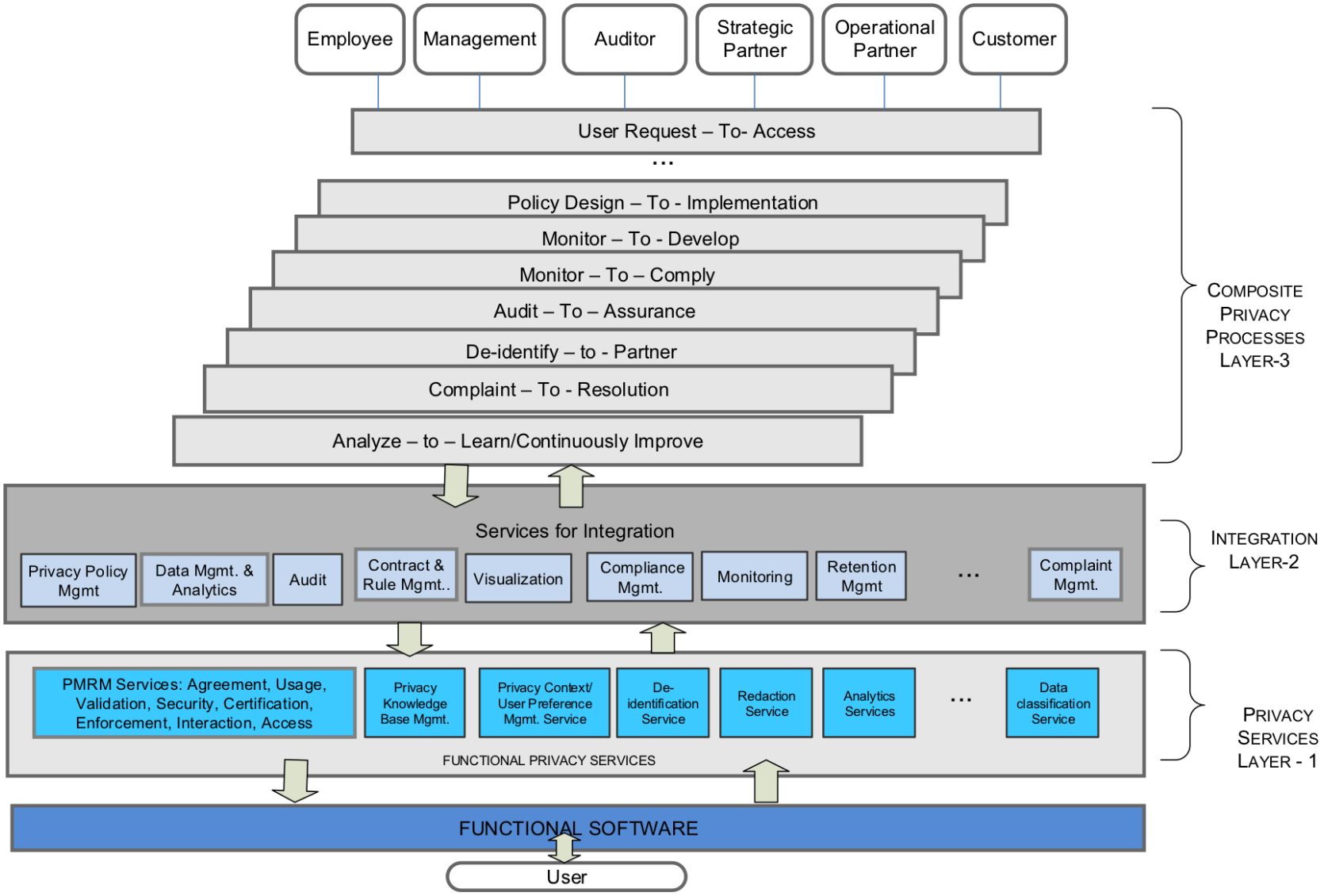
PbD "Sub-Principles"	*Compliance Criteria*	*Requirement(s)*
3. Privacy *Embedded* into Design		
3.1–Holistic and Integrative: Privacy commitments must be embedded in holistic and integrative ways	• Followed Privacy architectural design principles e.g. Comprehension (Visibility and Transparency), Consciousness (Awareness), Consent, Choice, Context (Locality etc.), Confinement, Consistency, Access, Security .. • Privacy Architecture easily integrated into functional architecture	• Documentation MUST include identification of privacy *architectural* design principles • Documentation MUST contain a Privacy Architecture • Documentation MUST contain description of the Business Model showing personal data flows for software services
3.2–Systematic and Auditable: A systematic, principled approach should be adopted that relies upon accepted standards and process frameworks, and is amenable to external review.	• Acknowledged software engineering process/methodology adopted • Privacy Metrics, e.g. effectiveness, monitored	• Documentation MUST identify the software engineering process/methodology used • Documentation SHOULD contain evidence of monitoring of privacy metrics
3.3–Review and Assess: Detailed privacy impact and risk assessments should be used as a basis for design decisions.	• Completed PIA and Risk Assessment • Completed Priority Matrix of Privacy Controls/Threats from Risk Analysis	• Documentation MUST contain a PIA • Documentation MUST contain Privacy Risk Assessment for use cases/user stories
3.4–Human-Proof: The privacy risks should be demonstrably minimized and not increase through use, misconfiguration, or error.	• Appropriate privacy failsafe mechanisms adopted	• Documentation MUST contain identification and description of privacy controls.

Privacy Architecture Design Principles: The 7 Cs

Comprehension **(User understanding of how PII is handled)**	**Users should *understand* how personal identifiable information (PII) is handled, who's collecting it and for what purpose, and who will process the PII and for what purpose across software platforms. Users are entitled to visibility - to know all parties that can access their PII, how to access/correct their own data, the limits to processing transparency, why the PII data is being requested, when the data will expire (either from a collection or database), and what happens to it after that. This category also includes legal rights around PII, and the implications of a contract when one is formed.**
Consciousness **(User awareness of what is happening and when)**	Users should be *aware* of when data collection occurs, when a contract is being formed between a user and a data collector, when their PII is set to expire, who's collecting the data, with whom the data will be shared, how to subsequently access the PII, and the purposes for which the data is being collected.
Choice **(To opt-in or out, divulge or refuse to share PII)**	Users should have *choices* regarding data collection activities in terms of opting in or out, whether or not to provide data, and how to correct their data.
Consent **(Informed, explicit, unambiguous)**	Users must first consent (meaning informed, explicit, unambiguous agreement) to data collection, use, and storage proposals for any PII. Privacy consent mechanisms should explicitly incorporate mechanisms of comprehension, consciousness, limitations, and choice.
Context **(User adjusting preferences as conditions require)**	Users should/must be able to *change privacy preferences* according to context. Situational or physical context—such as crowded situations (for example, when at a service desk where several people can listen in on your exchange when you provide a phone number, or when you are in the subway with cameras and audio on wearables around you)—is different from when you perform a buy transaction with Amazon.com or provide information to an app registered with an aggregator that sells to advertisers. Data also has context (such as the sensitivity of data, for example, financial and health data) could dictate different actions on the same PII in different contexts.
Confinement **(Data minimization, proportionality, and user-controlled re-use of data)**	Users must/should be able to *set/request limits* on who may access their PII, for what purposes, and where and possibly when/how long it may be stored. Setting limits could provide some good opportunities for future negotiation between vendors and users.
Consistency **(User predictability of outcome of transactions)**	Users should *anticipate with reasonable certainty* what will occur if any action in their PII is taken. That is, certain actions should be predictable on user access of giving out of PII.

Adapted from: Dawn N. Jutla, Peter Bodorik, "Sociotechnical Architecture for Online Privacy," IEEE Security and Privacy, vol. 3, no. 2, pp. 29-39, March-April 2005, doi:10.1109/MSP.2005.50. http://bit.ly/1qePUpn

PRIVACY ARCHITECTURAL BLUEPRINT



The Software Engineers' 1000 word models: Example Representations for Documentation

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

Spreadsheets

- Columns
  - Description of Personal Data/Data Cluster
  - Personal Info Category
  - PII Classification
  - Source
  - Collected by
  - Collection Method
  - Type of Format
  - Used By
  - Purpose of Collection
  - Transfer to De-Identification
  - Security Control during Data Transfer
  - Data Repository Format
  - Storage or data retention site
  - Disclosed to
  - Retention Policy
  - Deletion Policy
- DFDs
- Compare design options (identifiab-ility, linkab-ility, observab-ility)

4

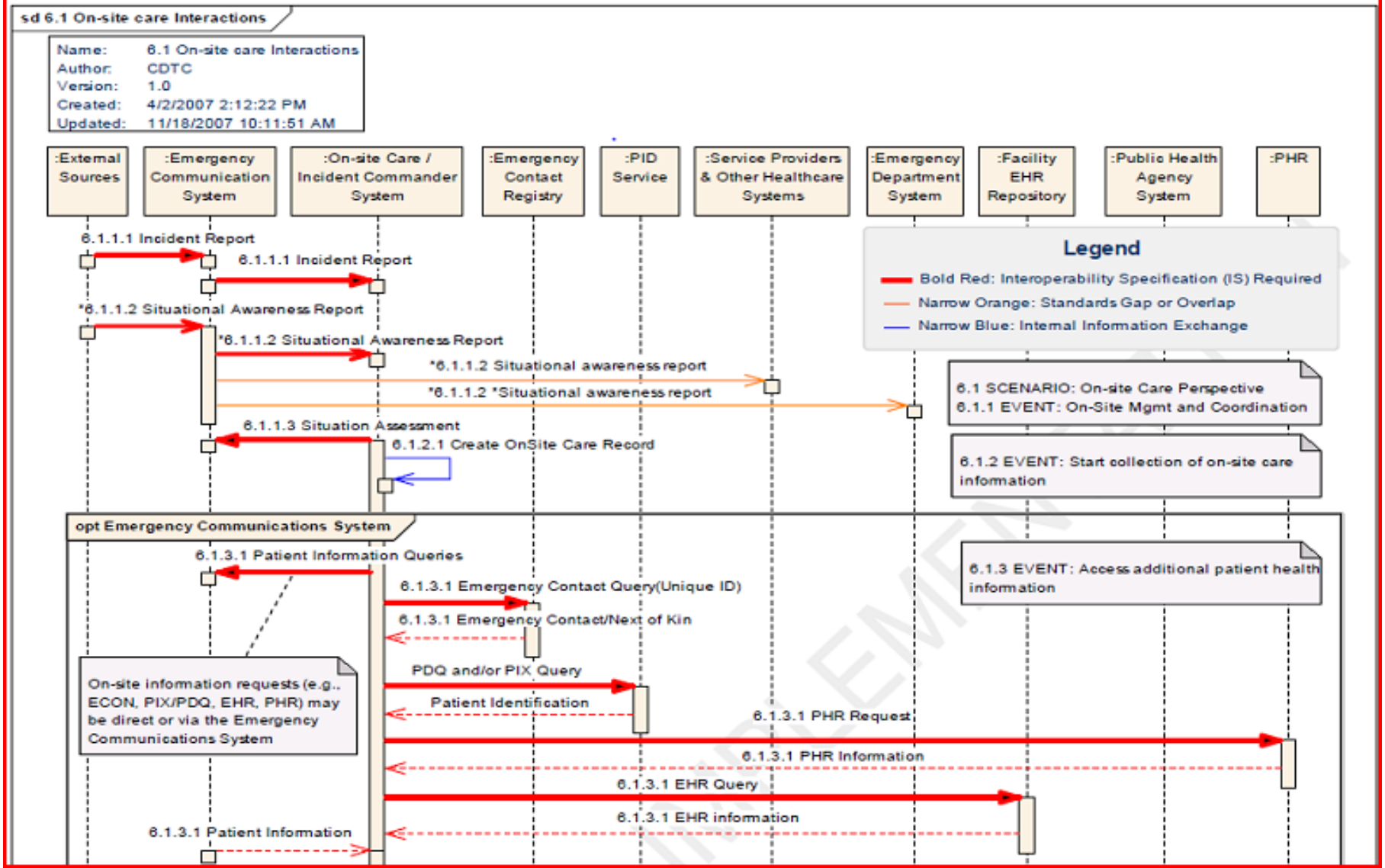
OASIS PMRM Methodology Step: For each actor instance, and incoming/outcoming data flow within a use case instance, (a) add context to requirements, and (b) determine the PMRM Services

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

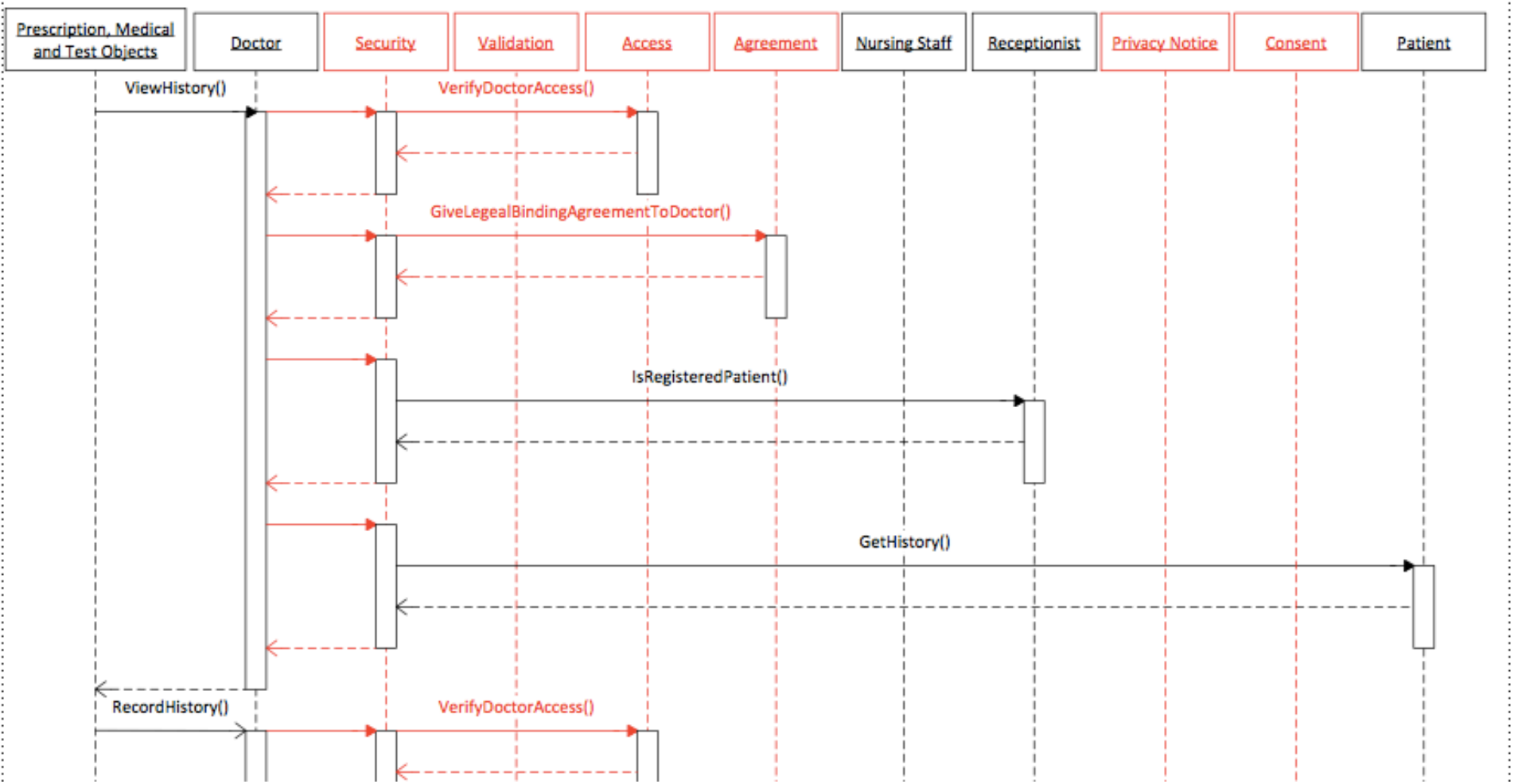
ACTOR: ECS	PI-In Incoming Data Flows	Actor Source	Requirements [Examples – Qualify with Context]	PMRM SVCs	[Context Narrative]	Comment
	Incident Report	External sources	• ECS Privacy and Security Policy • jurisdictional regulations • OnStar	• Security • Control • Audit • Interaction • Validation • Usage	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		

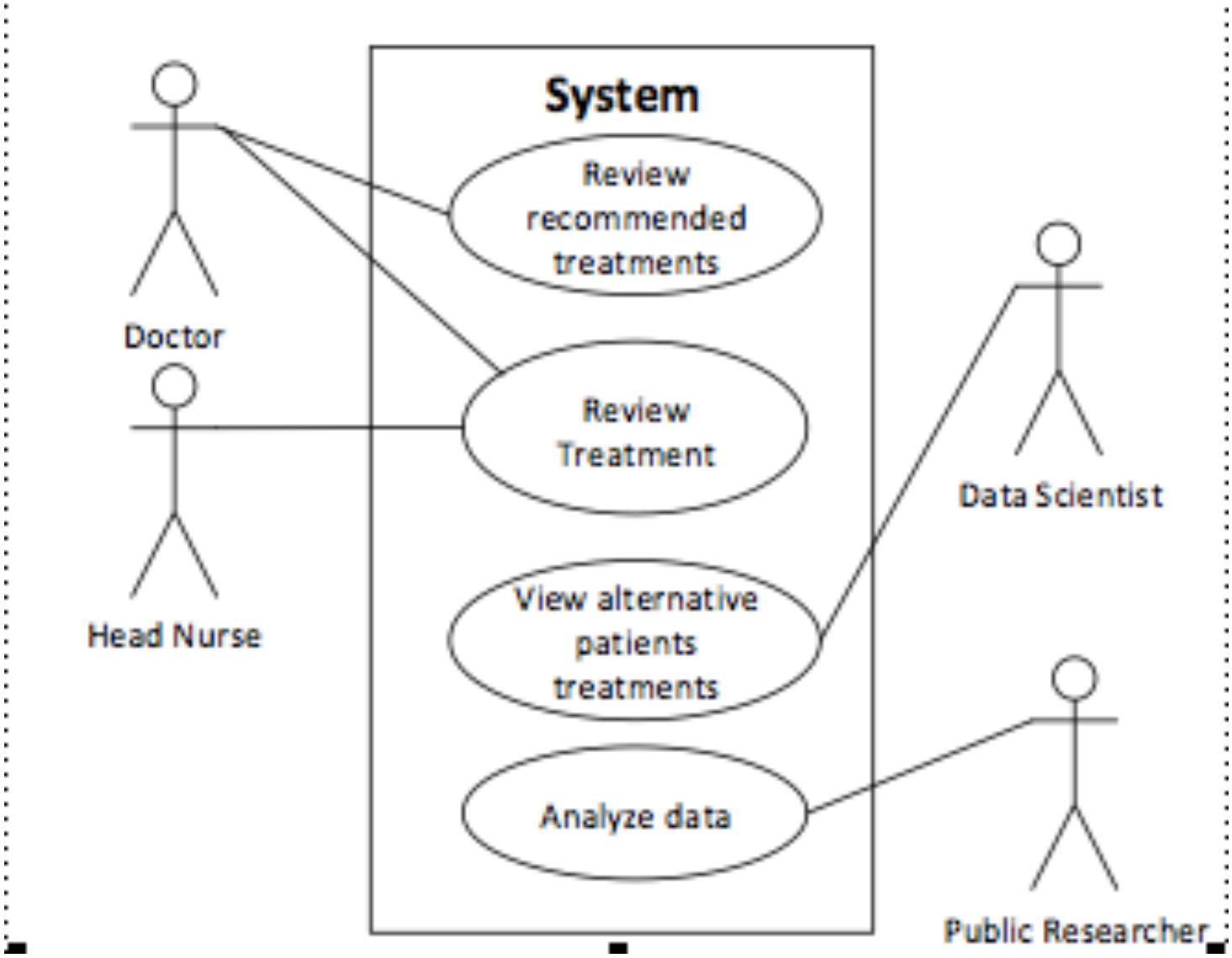
OASIS PMRM & PbD-SE Methodology Step: Describe the business processes and data flows using a data lifecycle description model and provide the level of detail needed to include <u>all actors and touch points</u>

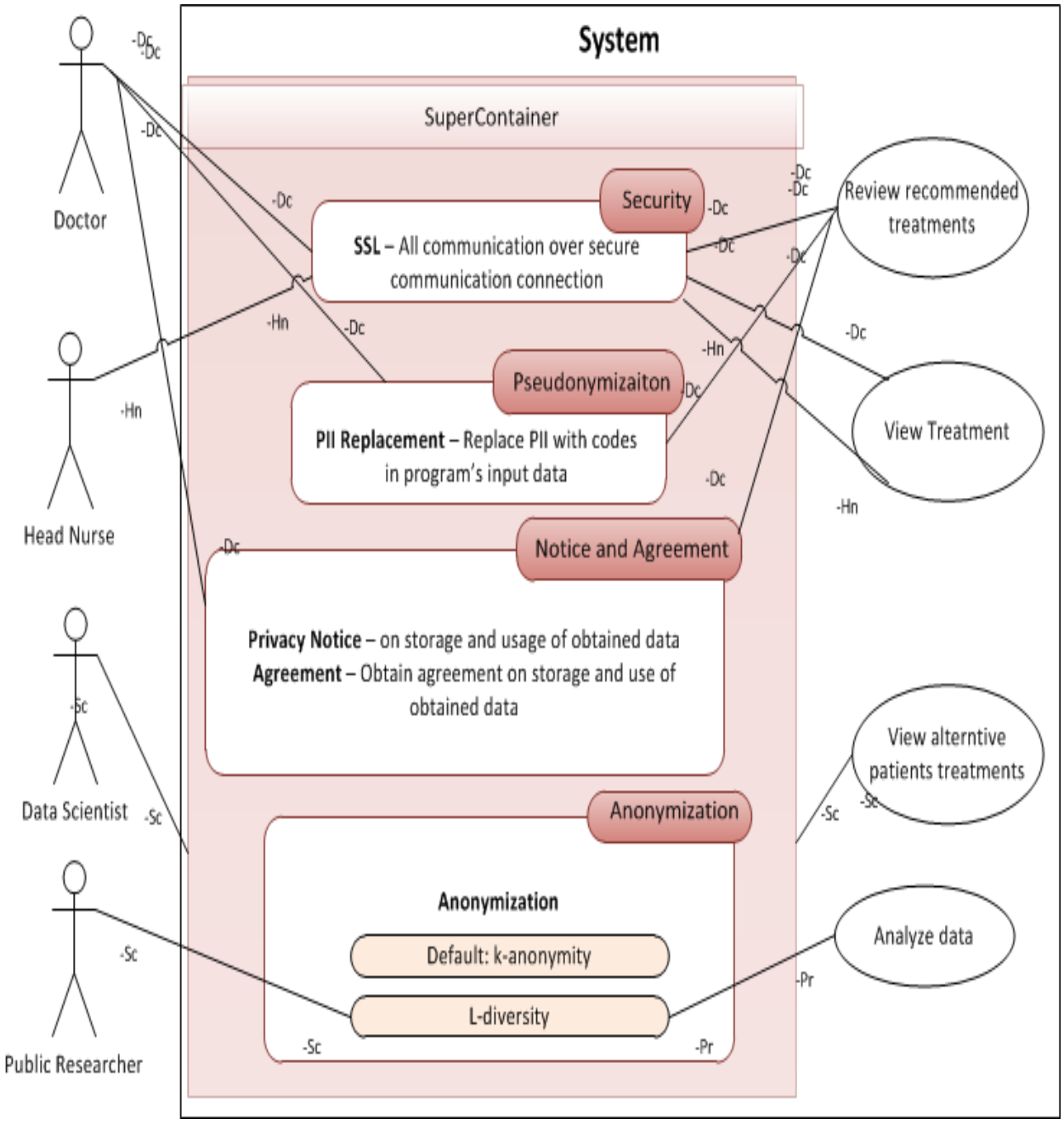
Figure 2.2.4.1-1 On-Site Care Scenario Perspective Business Sequence Diagram

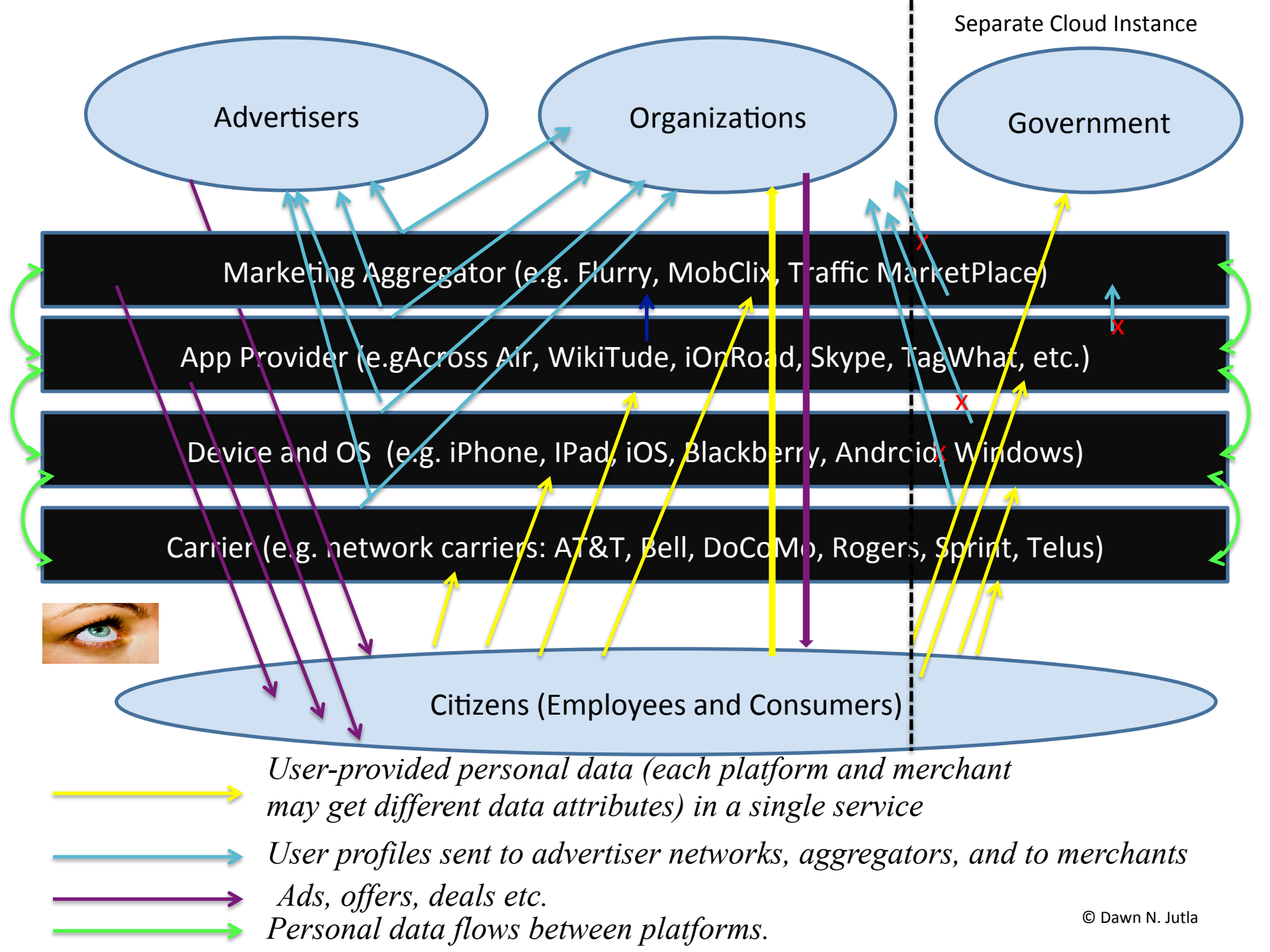


Visualizing Privacy Services in a UML Sequence Diagram




System
Review recommended treatments
Review Treatment
View alternative patients treatments
Analyze data
Doctor
Head Nurse
Data Scientist
Public Researcher


System
SuperContainer
Doctor
Head Nurse
Data Scientist
Public Researcher
Security
SSL – All communication over secure communication connection
Pseudonymizaiton
PII Replacement – Replace PII with codes in program's input data
Notice and Agreement
Privacy Notice – on storage and usage of obtained data
Agreement – Obtain agreement on storage and use of obtained data
Anonymization
Anonymization
Default: k-anonymity
L-diversity
Review recommended treatments
View Treatment
View alterntive patients treatments
Analyze data
-Dc
-Hn
-Sc
-Pr


Separate Cloud Instance
Advertisers
Organizations
Government
Marketing Aggregator (e.g. Flurry, MobClix, Traffic MarketPlace)
App Provider (e.gAcross Air, WikiTude, iOnRoad, Skype, TagWhat, etc.)
Device and OS (e.g. iPhone, IPad, iOS, Blackberry, Andrcid, Windows)
Carrier (e.g. network carriers: AT&T, Bell, DoCoMo, Rogers, Sprint, Telus)
Citizens (Employees and Consumers)
User-provided personal data (each platform and merchant may get different data attributes) in a single service
User profiles sent to advertiser networks, aggregators, and to merchants
Ads, offers, deals etc.
Personal data flows between platforms.

SAINT MARY'S UNIVERSITY
SOBEY
SCHOOL OF BUSINESS

Vision without Execution is Hallucination

Examples of such documentation exist across industries but not CONSISTENTLY

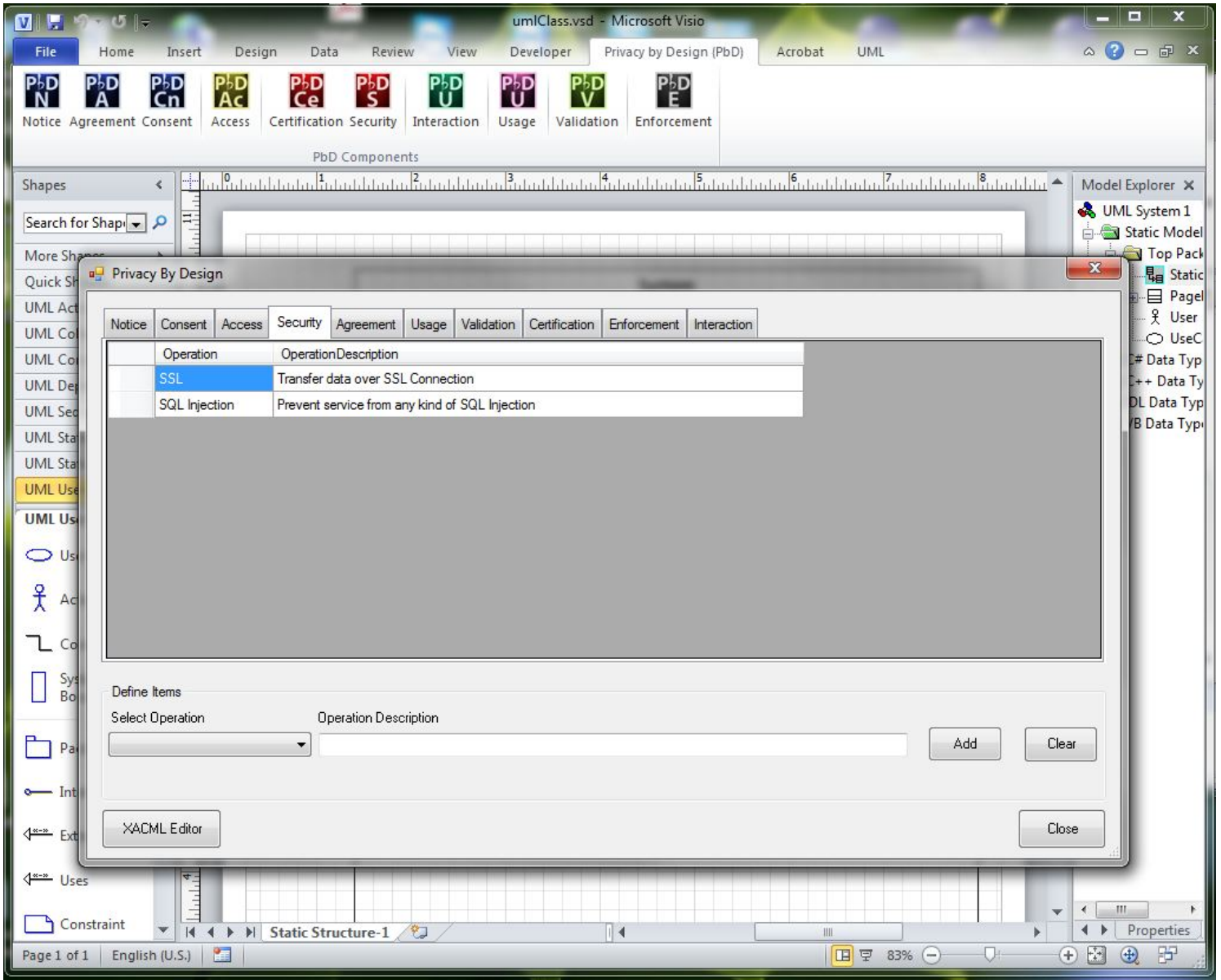
Roles of Education and Adoption

Institutionalize Privacy Engineering within Software Engineering
in Community College and University Programs
… in Computer Science, Engineering, Business, and the Arts

Create tools to make it EASIER for software engineers to comply to OASIS Emerging Privacy Standards without losing productivity

POSSIBLE FUTURE TOOLS IN SOFTWARE ENGINEERING EDUCATION/OASIS PbD-SE ADOPTION

SAINT MARY'S UNIVERSITY
SOBEY SCHOOL OF BUSINESS



SAINT MARY'S UNIVERSITY
SOBEY
SCHOOL OF BUSINESS

STATUS CHECK ON THE PRIVACY FIELD

Status:	IMMATURE
Progress:	TOO SLOW
Funding:	UNDERFUNDED
Priority:	COMPETING INTERESTS – (all stakeholders)
Risk:	CITIZENS LOSE ALL PRIVACY
Impact:	IMMEASURABLE in terms of the freedoms of future generations

A lot more time-consuming work to do …

Our changing societies with wearables, wireless, augmented reality, big data, and IoT machines communicating (M2M).

OASIS

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC