

Keynote Speech

SECURITY AND PRIVACY ON E-HEALTH APPLICATIONS

Youna Jung
Virginia Military Institute
jungy@vmi.edu



VIRGINIA MILITARY INSTITUTE
COMPUTER AND INFORMATION SCIENCES

Outlines

- ❑ Security on Online Applications
 - ✓ Basic Security
 - ✓ Security Mechanisms with XML-based Security Standards
- ❑ Privacy on Online Applications
 - ✓ Threats
 - ✓ Existing Solutions
- ❑ Privacy on e-Health applications
 - ✓ Challenges
 - ✓ Limitations and Requirements
- ❑ Privacy-Preserving Online Monitoring Framework

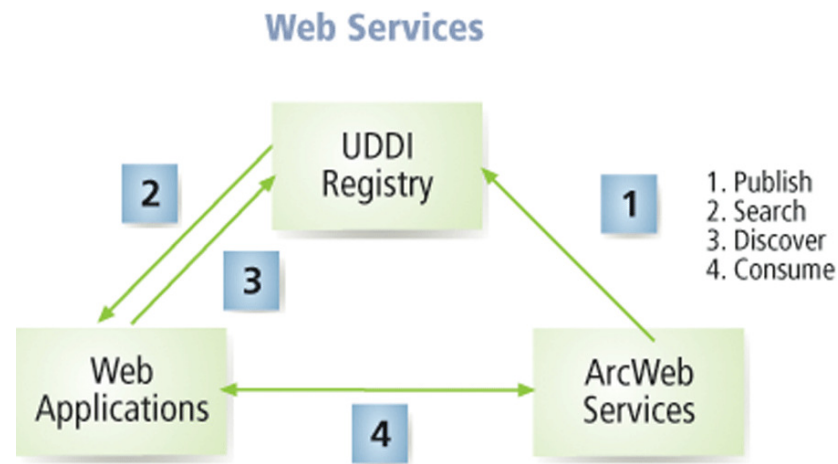
SECURITY ON ONLINE APPLICATIONS

Online Services

- ❑ require **end-to-end security** for transactions that span **multiple computers**.



- ❑ **Interoperability** become the most important to online services security
 - ✓ **Transmissions occur across multiple platforms** at all times.



Basic Security over HTTP

- ❑ Security methods outlined HTTP specification are **WEAK**
 - ✓ HTTP provides **NO** process for message **encryption**.



- ❑ **For stronger security**
 - ✓ HTTP security should be used **with other security technologies**
 - Ex) **SSL** and **Kerberos**.

XML based Security Standard

- ❑ Basic authentication and authorization techniques are **not sufficient to secure Web services transactions.**
- ❑ For better **interoperability** and **extensibility**
 - ✓ Need to mitigate the **security vulnerabilities of XML based applications**
 - XML-based applications raise significant security concerns
 - Because XML documents are encoded in **plan-text**, rather than in a binary form



Online services products use **a combination of security mechanisms implemented by using XML-based Security Standards**



1) XML Signature

- ❑ defines an XML syntax for digital signatures
 - ✓ Called XMLDSig, XML-DSig, or XML-Sig

```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK.../DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>...</SignatureValue>
  <KeyInfo>
    <KeyValue>
      <DSAKeyValue>
        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
      </DSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

2) XML Encryption

□ An example of XML Encryption

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- Fig. 12.3: Fig12_3.xml -->
<!-- XML file with the Personal element encrypted -->
- <Purchase xmlns="http://examplebookstore.com/purchase">
  <OrderNumber>99778866</OrderNumber>
  - <EncryptedData xmlns="http://www.w3.org/TR/xmlenc-core" Type="http://www.w3.org/TR/xmlenc-core#Element">
    <CipherData>
      <CipherValue>H3OI2J2MOII12J4NSAKJH2UIAJWI098128321JI78293M92310CDA9</CipherValue>
    </CipherData>
  </EncryptedData>
  <ItemNumber quantity="1">000459</ItemNumber>
</Purchase>
```



3) XML Key Management Specification (XKMS)

- ❑ XML specification for registering and distributing encryption keys for Public Key Infrastructure (PKI) in Web services.
 - ✓ developed by Microsoft, VeriSign and webMethods
 - ✓ designed for use with XML Signature and XML Encryption.

- ❑ XKMS is comprised of two specification
 - 1) XML Key Information Service Specification (X-KISS)
 - The set of **protocols** that process key Information
 - located in an **XML signature's Key-Info** element
 - 2) XML Key Registration Service Specification (X-KRSS)
 - The set of **certificate-management protocols** that addresses **the life of a digital certificate**
 - From registration to revocation and recovery.



4) Security Assertion Markup Language (SAML)

- ❑ An standard for transferring authentication, authorization and permissions information over the Internet.
- ❑ developed by combining two computing XML security standard
 - 1) Securant Technologies' AuthXML
 - 2) Netegrity's Security Services Markup Language (S2ML)
- ❑ Also provides a method for single sign-on authentication and authorization
 - ✓ SAML-based applications can provide single sign-on across disparate site and platforms.

5) Extensible Access Control Markup Language (XACML)

- ❑ A markup language that allows organizations to communicate their policies for accessing online information.
 - ✓ Developed by OASIS
 - ✓ defines
 - which clients can access information
 - what information is available to clients
 - when clients can access the information and
 - how client can gain access to information.

PRIVACY ON ONLINE APPLICATIONS

Created upon the presentation of Lorrie Faith Cranor
<http://lorrie.cranor.org>

Online Privacy Concerns

- ❑ Widespread Online Monitoring
 - Data is often **collected silently**
 - Web allows large quantities of data to be collected **inexpensively** and **unobtrusively**
- ❑ Re-identification of User Data
 - Data from multiple sources **may be merged**
 - Non-identifiable information can **become identifiable** when merged
- ❑ Misuse of Data
 - Data collected for business purposes may be **used in civil and criminal proceedings**
- ❑ Application-centric Privacy Management
 - Users given **no meaningful choice**

THREATS

1) Browsers

- ❑ Browsers provide information about
 - ✓ IP address, domain name, organization, Referring page,
 - ✓ Platform: O/S, browser
 - ✓ What information is requested
 - URLs and search terms
 - ✓ Cookies
- ❑ Disclose that information to anyone who might be listening
 - ✓ End servers
 - ✓ System administrators
 - ✓ Internet Service Providers
 - ✓ Other third parties
 - Advertising networks
 - ✓ Anyone who might subpoena log files later

2) Cookies

- ❑ Cookies can be **useful**
 - ✓ Used like **a staple to attach multiple parts** of a form together
 - ✓ Used to **identify you when you return** to a web site so you don't have to **remember a password**
 - ✓ Used to **help web sites understand how people use** them

- ❑ Cookies **can do unexpected things**
 - ✓ Used to **profile users and track their activities**, especially across web sites

Web Bug/Beacon

- ❑ Invisible “images” (1-by-1 pixels, transparent) embedded in web pages
 - ✓ cause referrer information and cookies to be transferred
 - ✓ Also called web beacons, clear gifs, tracker gifs, etc.

- ❑ Work just like banner ads from ad networks, but you can't see them unless you look at the code behind a web page

- ❑ To detect web bugs
 - ✓ ex) Bugnosis (<http://www.bugnosis.org>)

3) Data Merge

- ❑ Every time the same cookie is replayed to a site, the site may add information to the record associated with that cookie
 - ✓ Number of times you visit a link, time, date
 - ✓ What page you visit
 - ✓ What page you visited last
 - ✓ Information you type into a web form

- ❑ If multiple cookies are replayed together, they are usually logged together, effectively linking their data
 - ✓ Narrow scoped cookie might get logged with broad scoped cookie

4) Spyware

- ❑ Software that employs a user's Internet connection to collect information without their knowledge or explicit permission
 - ✓ Most products use pseudonymous, but unique ID
- ❑ Over 50% known freeware and shareware products contain Spyware
- ❑ Often difficult to uninstall!
- ❑ Anti-Spyware Sites
 - ✓ <http://grc.com/oo/spyware.htm>
 - ✓ <http://www.adcop.org/smallfish>
 - ✓ <http://www.spychecker.com>
 - ✓ <http://cexx.org/adware.htm>

5) Online Monitoring Service

- ❑ Provides **monitoring scripts** that enable online service providers to **track** and **record** users' characteristics, data entered, and actions.
 - ✓ *e.g.) mouse clicks, frequency of use, time spent in a particular page, media viewed, page navigation sequences, content entered into a textbox, location information, whether a mobile device is being used, and etc.*

- ❑ **Advantages**
 - 1) requires **less time and effort to collect and analyze** user/usage data
 - e.g.) *Google Analytics* and *Adobe Analytics*
 - 2) **widely used in** a variety of online application areas
 - e.g.) e-commerce, information retrieval, e-health, and etc.

SOLUTIONS

1) Privacy Policy

- ❑ Policies let consumers know about site's privacy practices
 - ✓ Consumers can then decide whether or not practices are acceptable
 - ✓ The presence of privacy policies increases consumer trust

- ❑ Privacy Policy Problem
 - ✓ difficult to understand
 - ✓ hard to find
 - ✓ take a long time to read
 - ✓ change without notice

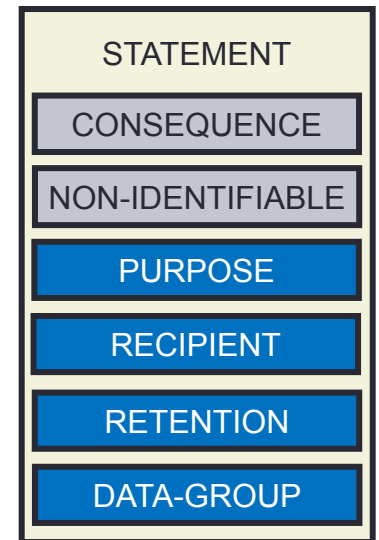
XML based Policy Languages

- ❑ Users and service providers can specify privacy preference.
 - ✓ Users - APPEL or XPref, Service providers - P3P
 - ✓ allow to describe
 - what kinds of user data might be monitored
 - what those data are used for
 - who those data will be shared with
 - how user data are maintained

Platform for Privacy Preferences (P3P)

- ❑ allows online applications to declare their privacy policies
 - ✓ data types to be collected (*Data*)
 - ✓ usage of collected data (*Purpose*)
 - ✓ consumers of user data (*Recipient*)
 - ✓ permanence (*Retention*)
 - ✓ accessibility of collected private data (*Access*)
 - ✓ dispute resolution procedure (*Disputes*)

- ❑ To specify data types
 - ✓ *Dynamic* data schema
 - to specify data that do not have fixed values
 - e.g.) *clickstream, http, clientevents, cookies, searchtext, and interactionrecord*
 - ✓ *User* data schema
 - to generally specify a user
 - E.g.) *name, bday, gender, home-info, business-info, and login*
 - ✓ *Third party* data schema
 - to provide third party information
 - its data types are identical to those of the *User* data schema
 - ✓ *Business* data schema
 - A subset of the *User* data relevant for describing legal policy entities.



Platform for Privacy Preferences (P3P)



A P3P Preference Exchange Language (APPEL)

- ❑ enables users to express their privacy preferences
- ❑ A complementary language to P3P
 - ✓ used by browsers to make automated decisions regarding the acceptability of P3P policies of applications.
- ❑ A user's policies are expressed in a set of *Ruleset*
 - ✓ A *RULE* consists of a policy (*p3p:POLICY*) and a behavior (*behavior*).

APPEL

```
<appel:RULESET xmlns:appel=http://www.w3.org/2002/04/APPELv1
  xmlns:p3p=http://www.w3.org/2000/12/P3Pv1
  crtddb="W3C" crtton="1999-11-03T09:21:32-05:00">
  <appel:REQUEST-GROUP>
    <appel:REQUEST uri="http://www.my-bank.com/*"/>
  </appel:REQUEST-GROUP>
  <appel:RULE behavior="limited" prompt="yes"
    description="Warning! Data may be shared.">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:RECIPIENT appel:connective="or" >
          <p3p:other-recipient/>
          <p3p:public/>
          <p3p:unrelated/>
        </p3p:RECIPIENT>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>
  ...
</appel:RULESET>
```

Behavior

- request
- block
- limited



XPref

- ❑ To overcome APPEL's drawbacks
 - ✓ keeps APPEL's rule heads
 - ✓ but replaces rule bodies with a condition attribute expressed by XPath

- ❑ Contributions of XPref
 - ✓ remove the ambiguity and complexity in APPEL's matching patterns
 - ✓ enhance its expression power

XPref

```
<RULESET>
```

Able to specify what is unacceptable!

```
<RULE behavior="block"
```

```
  condition="/POLICY/STATEMENT [ PURPOSE/* [ name(.) = "individual-analysis"]  
    and RECIPIENT/* [ name(.) != "ours" ] ]" />
```

```
<RULE behavior="request" condition="true"/>
```

```
</RULESET>
```

```
<RULESET>
```

Easy to express the acceptable combinations!

```
<RULE behavior="request"
```

```
  condition="/POLICY [
```

```
    every $stmt in $stmt/PURPOSE/*, every $purpose in @stmt/PURPOSE/*
```

```
    satisfies (name($purpose) = "current" or name($purpose) = "pseudo-analysis" or  
      (name($purpose) = "individual-analysis" and name($recip) = "ours")) ]"/>
```

```
<RULE behavior="block" condition="true"/>
```

```
</RULESET>
```



2) Privacy Guidelines

- ❑ Online Privacy Alliance
<http://www.privacyalliance.org>
- ❑ Direct Marketing Association Privacy Promise
<http://www.thedma.org/library/privacy/privacypromise.shtml>
- ❑ Network Advertising Initiative Principles
<http://www.networkadvertising.org/>
- ❑ OECD fair information principles
<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM>
- ❑ HIPAA
<https://www.hhs.gov/hipaa>

3) Seal programs

- ❑ The third-party assurance privacy certification programs for online applications
 - TRUSTe – <http://www.truste.org>
 - BBBOnline – <http://www.bbbonline.org>
 - CPA WebTrust – <http://www.cpawebtrust.org>



Seal programs

❑ Problems

- ✓ **Certify only compliance with stated policy**
 - Limited ability to detect non-compliance
- ✓ **Minimal privacy requirements**
- ✓ Don't address privacy issues that go beyond the web site
- ✓ Nonetheless, reporting requirements are forcing licensees to review their own policies and practices and think carefully before introducing policy changes

4) Software tools

Encryption tools

- ✓ prevent others from listening in on your communications
 - File encryption
 - Email encryption
 - Encrypted network connections

Filters

- ✓ Cookie cutters
- ✓ Child protection software

Anonymity tools

- ✓ prevent your actions from being linked to you
 - Anonymizing proxies
 - Mix Networks and similar web anonymity tools
 - Anonymous email

Provider-side Privacy Protection

❑ Adchoices

- ✓ Third-party advertising companies have voluntarily begun to **insert an 'Adchoices' icon** into their ads
 - to increase user awareness of online tracking.

But it has been found that the icon **was not very effective**

❑ Privad

- ✓ A **middleware** approach
- ✓ to conceal a user's activities from an advertising network by

Huge overhead requirements

→ The adoption of a proxy-based middleware may not be a feasible solution to small-size e-health applications

Useless

- if an e-health application requires identifiable user data



User-side Protection: Browser-based

❑ Adnostic

- ✓ A browser extension
- ✓ behavioral profiling and targeting in users' browsers
 - to select effective ads while not sending user data to third-party ad companies.

❑ RePriv

- ✓ enables browsers to conduct user interest mining
- ✓ only share the resulting encapsulated interests with third-parties

Both have only focused on targeted advertising and personalization
but have **NOT considered online monitoring services.**

User-side Protection: Browser-based

- ❑ opt-out cookies
 - ✓ A simple and easy-to-use solution

Fragile

- they can be **easily disabled or deleted** by a third party

- ❑ Setting a block list in a browser
 - ✓ can effectively block malicious applications

Not support fine-grained blocking at the data level

- currently this approach blocks any listed application in its entirety and does

User-side Protection: Policy-based

□ Privacy Bird

- ✓ A P3P user agent
 - reads P3P policies of online applications and lets users know whether the application policies and user preferences are matched.
 - If policies are not matched, a bird icon turns red.
- ✓ A user can get information by clicking on a red bird icon.

Not allow users to check data being monitored at the data level and **Not prevent unauthorized monitoring.**

- only able to check the acceptability of application's P3P policies

SECURITY AND PRIVACY ON E-HEALTH

Online Monitoring on e-Health Applications

❑ Application Domains

- ✓ Online healthcare education [10]
- ✓ Healthcare research [11]
- ✓ Healthcare interventions
- ✓ Disease prevention and self-management
- ✓ Health promotion [13]

❑ Major Functionalities

- ✓ Self-assessment or self-profiling
 - to recognize individuals' health-related status
 - → provide personalized healthcare services
- ✓ Continuous communication with patients using interactive tools
 - e.g.) online trackers
- ✓ Wide dissemination of information related to health and safety

Detailed monitoring is critical

- to provide personalized healthcare services
- to confirm that e-health apps are used correctly
- ← Need to collect detailed, and often identifiable, user data including health information.



Protection of user privacy is critical

- e-health applications often deal with very sensitive private data, including health status, medical records, and family health histories.
- Control over the sharing of this information is of the utmost importance and urgency

Requirements for e-Health applications

- ❑ Privacy policy on patients' health data → [Health Data Schema](#)
- ❑ Online monitoring services that are aware of user privacy policies rather than application policies → [PPoM Service](#)
- ❑ Verification methods to ensure that an application complies with policies mutually agreed by providers and users on user side → [PPoM Browser](#)
- ❑ Enforcement methods to protect user privacy on user side
- ❑ Easy-to-use tools → [PPoM Tool](#)



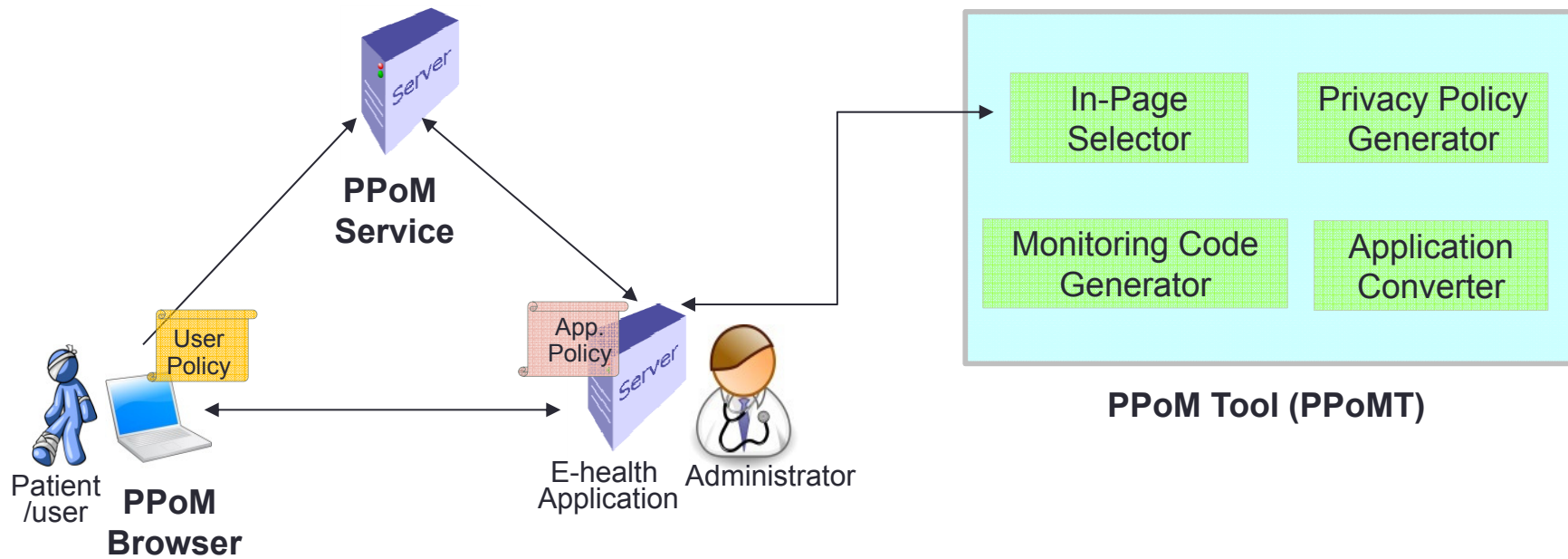
Privacy-Preserving online Monitoring (PPoM)

- allows e-health applications to conduct trustworthy user monitoring
- enable patients to use e-health applications without privacy loss

PRIVACY-PRESERVING ONLINE MONITORING

PPoM Framework

Overall Architecture



1. Health Data Schema

- ❑ To avoid having inconsistent schemas across different patients and applications
- ❑ aims to describe a patient's health status



HIPAA-compliant Privacy Policy

- ❑ An extension of P3P to be a HIPAA-friendly policy language
 - ✓ Privacy policy language to be used in e-health applications must

Proposed P3P Extension	HIPAA
<p><ACCESS></p> <p>Existing: <nonident/>, <all/>, <none/>, <contact-and-other/>, <ident-contact/>, and <other-ident/>.</p> <p>Addition: <HIPAA-compliant-access/></p>	<p>HIPAA 164.524: A patient’s access rights compliant with HIPAA can be represented <HIPAA-compliant-access/>.</p>
<p><DEIDENTIFIED></p> <p>Addition: This element is a new child element of <STATEMENT> and it is optional.</p>	<p>HIPAA 164.502: <DEIDENTIFIED> must be specified in case of policies for de-identified PHI.</p>
<p><PURPOSE></p> <p>Existing: <current/>, <admin/>, <develop/>, <tailoring/>, <contact/>, <historical/>, <pseudo-analysis/>, <pseudo-decision/>, <telemarketing/>, <individual-analysis/>, <individual-decision/>, and <other-purpose/>.</p> <p>Addition: <public-health/>, <research/>, <healthcare-operation/>, and <healthcare-reference/></p>	<p>HIPAA 164.514: Health/HIIPAA-related purposes can be represented using newly added four purposes.</p>

Proposed P3P Extension	HIPAA
<p><RECIPIENT></p> <p>Existing: <ours>, <delivery>, <same>, <other-recipient>, <unrelated>, and <public>.</p> <p>Addition: <user> and <limited-dataset-recipient></p>	<p>Across HIPAA regulations: 'Covered entity' in HIPAA is represented as <ours> 'Limited data set recipient' in HIPAA is represented as < limited-dataset-recipient ></p>
<p><RETENTION></p> <p>Existing: <no-retention/>, <stated-purpose/>, <legal-requirement/>, <business-practices/>, and <indefinitely/>.</p> <p>Addition: <HIPAA-compliant-retention/></p> <p>Modification: <RETENTION> has two optional attributes, <i>expiry-date</i> and <i>expiry-event</i>.</p>	<p>HIPAA 164.502: An e-health application can represent HIPAA-abiding retention policy using <HIPAA-compliant-retention> HIPAA 164.508: An e-health application can represent expiry dates and events of PHI using 'expiry-date' and 'expiry-event'.</p>
<p><DATA></p> <p>Existing: Categories are <health/>, <physical/>, <online/>, <uniqueid/>, <purchase/>, <financial/>, <computer/>, <navigation/>, <interactive/>, <demographic/>, <content/>, <state/>, <political/>, <preference/>, <location/>, <government/>, and <other-category/>.</p> <p>Addition: The <i>Health</i> data schema to be referred</p>	<p>Across HIPAA regulations: For health data, we should specify <health/> as a data category. In addition, a value of a <i>ref</i> attribute of a <DATA> must start with "#health" to refer the Health data schema.</p>

2. PPoM Service

- ❑ gathers only authorized data that users allow to monitor.
 - ✓ By specifying user policies, patients can determine which data can be monitored → User policies are enforced by the PPoM service.

[ELEMENT_ID|ELEMENT_PATH] [EVENT_TYPE] [TIME] [DATA_TYPE] [DATA]
[DEVICE_INFORMATION]

- *ELEMENT_ID*: It is a unique ID of a HTML element.
- *ELEMENT_PATH*: In case of dynamic webpages, a path from the root element is used as an ID if an element does not have ID. The path is unique for each element.
- *EVENT_TYPE*: It denotes that a type of an event occurred. The set of event types are as follows: {*entering a page, leaving a page, clicking an element, filling an element*}.
- *TIME*: It denotes the occurring time of an event
- *DATA_TYPE*: It is a type of monitoring data and must be specified based on the data types in the P3P data schema and the HIPAA Profile.
- *DATA*: It is the value of the monitoring data.
- *DEVICE_INFORMATION*: It includes a device's *category, operating system, language, and browser information*.

3. PPoM Browser

- 1) understands user policies, 2) presents all data being monitored, and 3) protects user privacy on the user side by blocking outgoing messages which contain data a user does not want to disclose.

Tell Us About You

To get started please tell us your health status

Current Weight: pounds [switch to metric](#)

Height: feet inches

Blood Type:

Disease:

How Active Are You?

Sedentary: I have a desk job and/or sit most of the day (secretary, computer)

Lightly Active: I stand a lot of the day (nurse, teacher)

Active: I move around a lot throughout the day (courier, waiter)

[Click to Continue](#)

- Height
- Weight
- Hearing Acuity
- Visual Acuity
- Blood Type
- Blood Pressure
- Blood Sugar Level
- Cholesterol Level
- Disabilities
- Allergies
- Lab Tests
- Medication
- Disease History
- Family Medical History
- Immunization History
- Healthcare Provider

Dynamic ▲ ● User ▲ ● Business ▲ ● Third Party ▲ ● Health ▼

4. PPoMT

- helps non-IT health professionals specify privacy policies and easily convert their existing applications into privacy-preserving applications.

Tell Us About You

To get started please tell us y

Current Weight:

Height: feet

Blood Type:

Disease:

How Active Are You

Sedentary: I have a

Lightly Active: I stan

Active: I move aroun

[Click to Continue](#)

Privacy Policy For TextBox (#txtDisease)

Consequence

Purpose

<input type="checkbox"/> <current/>	<input type="checkbox"/> <admin/>	<input type="checkbox"/> <develop/>	<input type="checkbox"/> <tailoring/>
<input type="checkbox"/> <contact/>	<input type="checkbox"/> <historical/>	<input type="checkbox"/> <pseudo-analysis/>	<input type="checkbox"/> <pseudo-decision/>
<input type="checkbox"/> <telemarketing/>	<input type="checkbox"/> <individual-analysis/>	<input type="checkbox"/> <individual-decision/>	<input type="checkbox"/> <other-purpose/>
<input type="checkbox"/> <public-health/>	<input checked="" type="checkbox"/> <research/>	<input checked="" type="checkbox"/> <healthcare-operation/>	<input type="checkbox"/> <healthcare-reference/>

Non-Identifiable

Yes No

Recipient

<input checked="" type="checkbox"/> <ours/>	<input type="checkbox"/> <delivery/>	<input type="checkbox"/> <same/>	<input type="checkbox"/> <other-recipient/>
<input type="checkbox"/> <unrelated/>	<input type="checkbox"/> <public/>	<input type="checkbox"/> <limited-dataset-recipient/>	

Retention


<input type="checkbox"/> <no-retention/>	<input type="checkbox"/> <stated-purpose/>	<input type="checkbox"/> <legal-requirement/>	<input type="checkbox"/> <business-practices/>
<input type="checkbox"/> <indefinitely/>	<input checked="" type="checkbox"/> <HIPAA-compliant-retention/>		

Data

<input checked="" type="checkbox"/> <health/>	<input type="checkbox"/> <physical/>	<input type="checkbox"/> <online/>	<input type="checkbox"/> <uniqueid/>
<input type="checkbox"/> <purchase/>	<input type="checkbox"/> <financial/>	<input type="checkbox"/> <computer/>	<input type="checkbox"/> <navigation/>
<input type="checkbox"/> <interactive/>	<input type="checkbox"/> <demographic/>	<input type="checkbox"/> <content/>	<input type="checkbox"/> <state/>
<input type="checkbox"/> <political/>	<input type="checkbox"/> <preference/>	<input type="checkbox"/> <location/>	<input type="checkbox"/> <other-category/>
<input type="checkbox"/> <government/>	<input type="checkbox"/> <government/>		

Health Data Scheme

<input type="radio"/> height	<input type="radio"/> weight	<input type="radio"/> hearing-acuity	<input type="radio"/> visual-acuity
<input type="radio"/> blood-type	<input type="radio"/> blood-pressure	<input type="radio"/> blood-sugar-level	<input type="radio"/> cholesterol-level
<input type="radio"/> disabilities	<input type="radio"/> allergies	<input type="radio"/> lab-tests	<input type="radio"/> medication
<input checked="" type="radio"/> disease-history	<input type="radio"/> family-medical-history	<input type="radio"/> immunization-history	<input type="radio"/> andhealthcare-providers



VIR
COMF

a Jung

Conclusion

- ❑ Security and privacy is one of the critical issues on e-Health applications
- ❑ For widespread use of e-health applications
 - ✓ Must provide proper methods for the security, especially for privacy preservation
 - ✓ Otherwise, people may keep hesitating to use e-health applications.
- ❑ Need to stay apprised of all security developments and update their systems regularly.

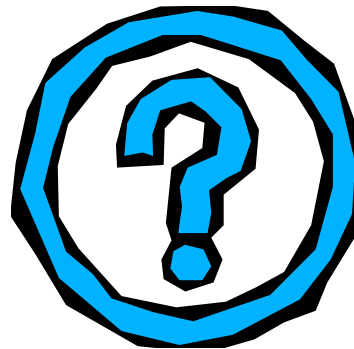
References

- ❑ Youna Jung, “Toward Usable and Trustworthy Online Monitoring on e-Health Applications”, *International Journal on Advances in Life Science*, IARIA, Vol. 8 No. 1 & 2, pp. 122-132, 2016.
- ❑ Youna Jung and Minsoo Kim, “HIPAA-Compliant Privacy Policy Language for e-Health Applications”, the 6th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2016), Elsevier, September 19-22, London, United Kingdom, 2016 [In Press].
- ❑ Youna Jung and Minsoo Kim, “A Developemnt of Privacy-Preserving Monitoring System for e-Health Applications”, the 5th international conference on global health challenges (Global Health 2016), IARIA, October, 2016 [In Press].
- ❑ Mark S. Ackerman, Lorrie Faith Cranor and Joseph Reagle, *Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy*, (AT&T Labs, April 1999), <http://www.research.att.com/projects/privacystudy/>
- ❑ Mary J. Culnan and George R. Milne, *The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses*, (December 2001), <http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf>.
- ❑ Cyber Dialogue, *Cyber Dialogue Survey Data Reveals Lost Revenue for Retailers Due to Widespread Consumer Privacy Concerns*, (Cyber Dialogue, November 7, 2001), <http://www.cyberdialogue.com/news/releases/2001/11-07-uco-retail.html>.
- ❑ Forrester Research, *Privacy Issues Inhibit Online Spending*, (Forrester, October 3, 2001).

References

- ❑ Louis Harris & Associates and Alan F. Westin, *Commerce, Communication and Privacy Online* (Louis Harris & Associates, 1997),
<http://www.privacyexchange.org/iss/surveys/computersurvey97.html>
- ❑ Louis Harris & Associates and Alan F. Westin. E-Commerce and Privacy, *What Net Users Want*, (Sponsored by Price Waterhouse and Privacy & American Business. P & AB, June 1998).
<http://www.privacyexchange.org/iss/surveys/ecommsum.html>
- ❑ Opinion Research Corporation and Alan F. Westin. “Freebies” and Privacy: What Net Users Think. Sponsored by Privacy & American Business. P & AB, July 1999.
<http://www.privacyexchange.org/iss/surveys/sr990714.html>
- ❑ Privacy Leadership Initiative, *Privacy Notices Research Final Results*, (Conducted by Harris Interactive, December 2001),
<http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf>
- ❑ *An extensive list of privacy surveys from around the world is available from*
<http://www.privacyexchange.org/iss/surveys/surveys.html>.

Questions?



Send an email to jungy@vmi.edu