



# Cementing the Privacy Foundation of Information Technology

**eHealth 2015 – June 1, 2015**

Robin Gould-Soil, CPO, ConnectingGTA, University Health Network

Natalie Comeau, Supervisor, Privacy Advisory Services, University Health Network



# Experience

## ConnectingGTA

## Patient Portals



The screenshot shows the myUHN patient portal sign-in interface. At the top left is the myUHN logo. Below it is a 'SIGN IN' section with a 'Username' field containing 'bentuhn@hotmail.com' and a 'Password' field with masked characters. A blue 'Sign In' button is positioned below the password field, with a link 'Forgot your username or password?' underneath. A 'How to Register' button is located below the sign-in form. To the right of the form is a photograph of a woman in a pink shirt smiling while using a laptop. Below the photo, text states: 'With myUHN Patient Portal, you will be able to:' followed by a bulleted list: 'View UHN appointments', 'View UHN test results, reports, discharge summaries and clinic notes', and 'Share information with others'. A link 'Learn how UHN protects your privacy.' is provided. The footer contains contact information, copyright notice for 2014 University Health Network, and the UHN logo with the slogan 'COURAGE LIVES HERE' and the names of the four hospitals: Toronto General, Toronto Western, Princess Margaret, and Toronto Rehab.



# Iterative PbD Processes

- Patient / Clinical Working Group define and prioritize requirements (Business Requirements Doc – BRD)
- Privacy / Technical SMEs & Working Groups vet and add to the BRD
- BRD translated into RFP
- After vendor selected, end users, technical staff, privacy experts continue to develop requirements, considering resource constraints & each other's needs
  - Legal compliance
  - Technical feasibility
  - Timelines & priorities
- Prototypes and mockups used to demonstrate functionality to all working groups and Steering Committees for acceptance
  - Healthcare Human Factors creation
  - Patient Usability sessions
- Final decisions reviewed with all working groups, based on acceptance criteria and demonstrations of functionality

## Privacy by Design Principles

- **Proactive not Reactive – Preventative not Remedial**
- **Privacy as the Default Setting**
- **Visibility & Transparency – Keep it Open**

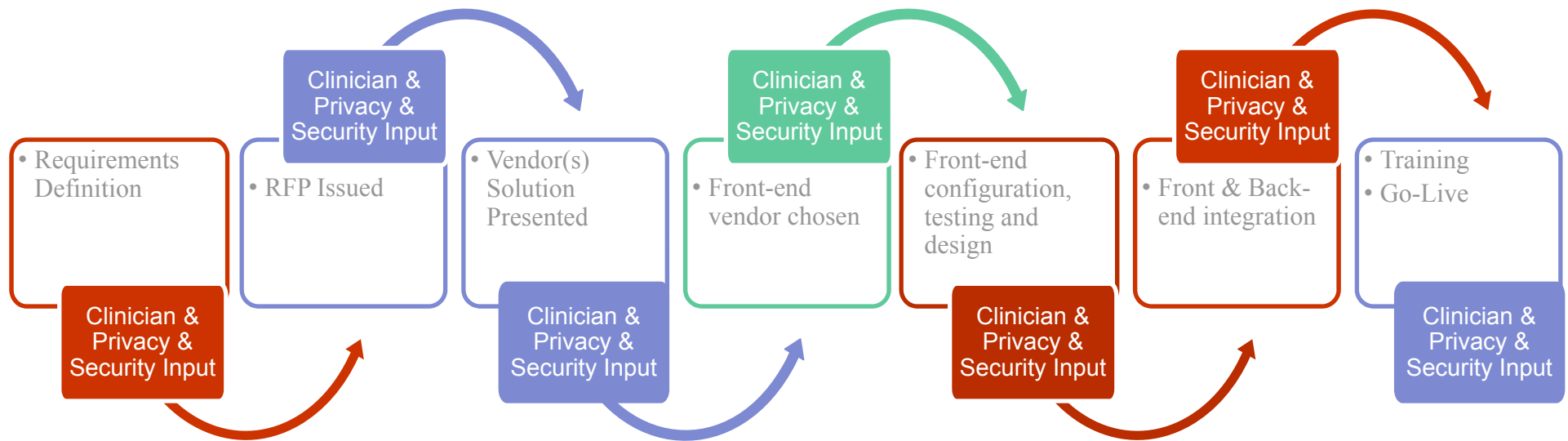
# Iterative Design Experience



© 2009/10/10

# Iterative Design Experience - ConnectingGTA

- Highly engaged groups: vendor, Clinical Working Group, Technical Working Group, Privacy & Security Working Group, program privacy and security specialists



# Privacy Engagement Options

- Casual, automatic engagement – project team maturity
- Mapped against other similar systems (US and Canada)
  - E.g. terms of use, authentication & registration, proxys
- Environmental scan by students / contractors
  - E.g. Clarified patient desires and needs, identified need for culture change
- Conducted right type of PIA
  - Conceptual – when have concept only and need to know what to include (e.g. social media principles? children’s consent?)
  - Logical & physical - when have technology design done (don’t forget manual processes)
  - Technical – when legislative authority is clear but flow of data / technology should use up-to-date best practices (E.g. reference COACH Privacy and Security for Patient Portal Guidelines)
- Document using PIA / document using project processes
  - Requirements, policies, decisions



# ConnectingGTA – Comprehensive & Secure Patient Search



<p>Find the right patient.</p> <p>Find a patient with a unique # (OHIP or MRN)</p> <p>Find a patient in an emergency (no unique #)</p>	<p>Support searching with unique ID, MRN, OHIP, name, date of birth, gender</p>	<p>Possible:</p> <ul style="list-style-type: none"> <li>• different combinations of fields</li> <li>• some or all fields mandatory</li> </ul>	<ul style="list-style-type: none"> <li>✓ Include enough PHI for positive identification</li> <li>✓ Use no more PHI than necessary</li> <li>✓ Only return 1 patient whenever possible</li> </ul>	<p>Clinicians can do 1 of 3 searches:</p> <ol style="list-style-type: none"> <li>1. OHIP &amp; name &amp; gender</li> <li>2. MRN &amp; org name</li> <li>3. Advanced Search (any of name, DOB, gender, address)</li> </ol> <p>No information displayed if more than 5 results match</p>
--	---	---	---	---



1

Patient Search and Selection

Search by HCN   Search by MRN/CHRIS Client #   Advanced Search

HCN (Ontario Only) \*required   Gender \*required   Last Name \*required

2

Patient Search and Selection

Search by HCN   Search by MRN/CHRIS Client #   Advanced Search

Organization \*required   MRN/CHRIS Client # \*required

3

Patient Search and Selection

Search by HCN   Search by MRN/BRN   Advanced Search

Last Name   First Name   Middle Name

DoB (DDMMYYYY)   Gender

Street Address   City   Postal Code   Phone Number (e.g., 416-123-4567)

Organization



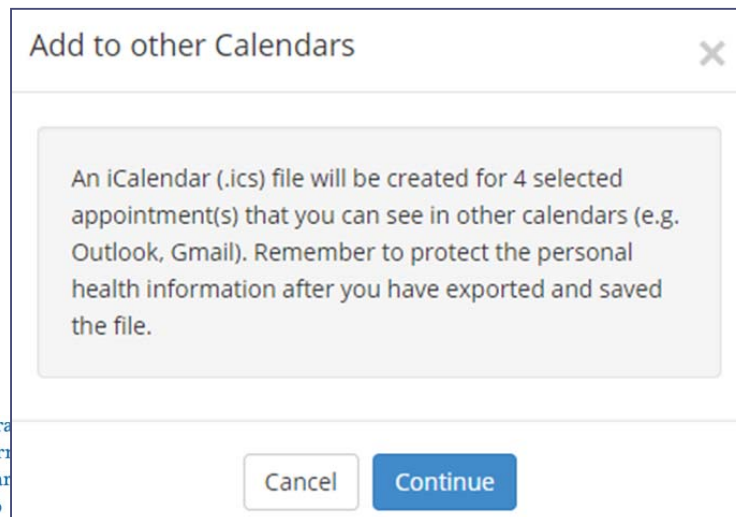
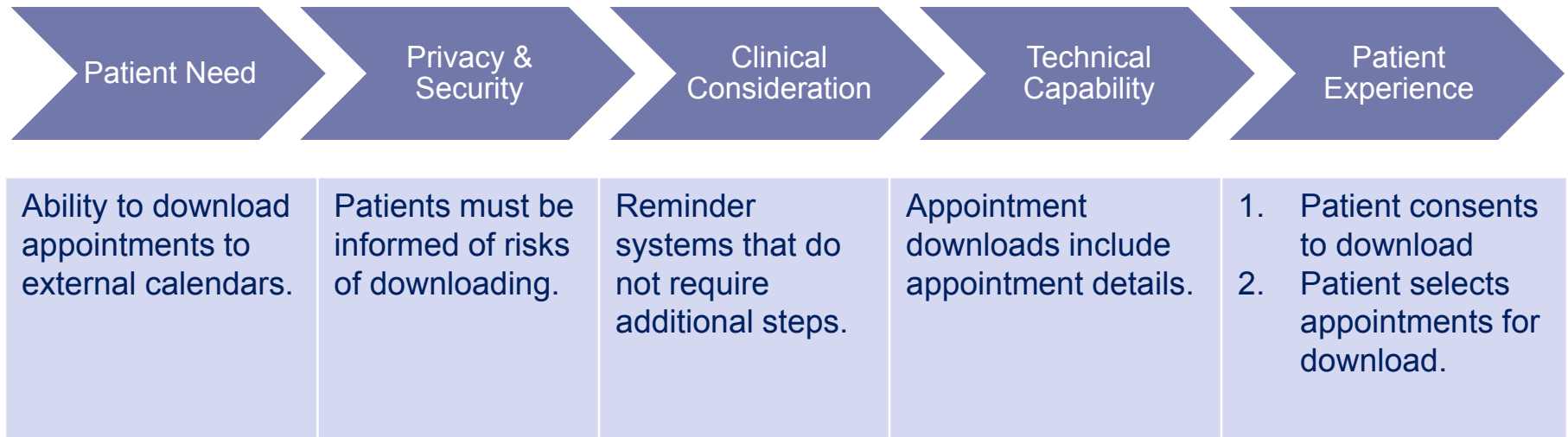
# Lessons Learned – Designing Patient Search

- Requiring a match of 3 identifiers may prevent ‘fishing trips’ but do not work in outlying scenarios, such as emergencies
  - Ensure meet the variety of clinical scenarios
  - Add in controls: Limit search results to reduce PHI ‘leak’/exposure
- Patience! Design phase took 3 cycles of iteration between Privacy and Security Working Group, Clinical Working Group and vendor

Privacy by Design  
Principle #4

**Full  
Functionality–  
Positive Sum,  
not Zero Sum**

# Patient Portals – Downloading Appts



# Lessons Learned – Designing Downloading Appts

- Layered notices and reminders
  - Terms of use / examples upon set up
  - Additional safeguards (behaviours) patients can take described in Terms of Use
- Patients said they want the ability to choose, and to turn on and OFF!

Privacy by Design  
Principle #5

End-to-End  
Security – *Full  
Lifecycle  
Protection*

# Top 10 Lessons Learned

1. Integrate privacy team into each step and process
2. Build a strong, documented governance model that outlines decision making authority, and escalation points
3. Put end users first!
4. Iterate!
5. Identify standards and methodologies that can be referenced
6. If little written industry standard or internal policy, look to environmental scans & daily practices
7. Test and Learn
8. Build for the future (e.g. standard data feeds)
9. Be prepared for changes in the future (as measure impacts to patient rights & clinical care)
10. PIA is a wrapper for external stakeholders



# Thank You!

Robin Gould-Soil, CPO

[Robin.gould-soil@uhn.ca](mailto:Robin.gould-soil@uhn.ca)

416-340-4800 ext. 6620

Natalie Comeau, Supervisor, Privacy Advisory Services

[Natalie.comeau@uhn.ca](mailto:Natalie.comeau@uhn.ca)

647-539-4636

