Cementing the Privacy Foundation of Information Technology

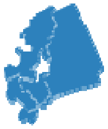
eHealth 2015 – June 1, 2015

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

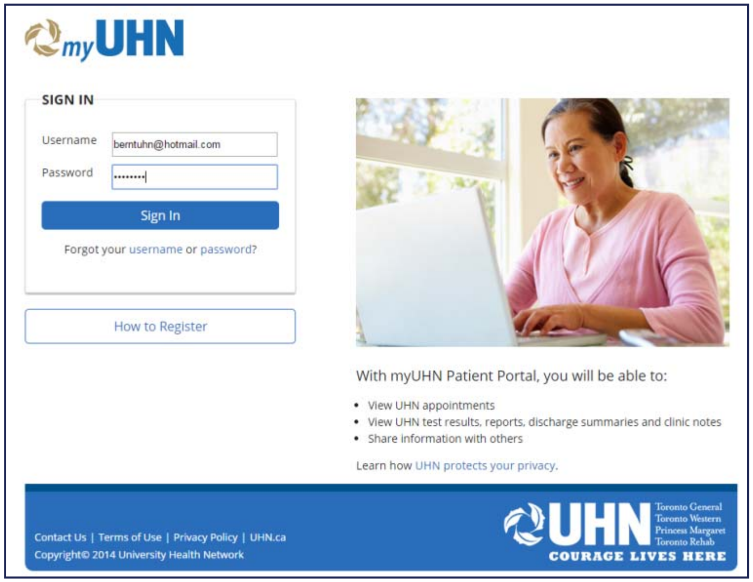
Natalie Comeau, Supervisor, Privacy Advisory Services, University Health Network

Experience

ConnectingGTA



Patient Portals



myUHN

SIGN IN

Username bemtuhn@hotmail.com

Password ••••••••

Forgot your username or password?

With myUHN Patient Portal, you will be able to:

- View UHN appointments
- View UHN test results, reports, discharge summaries and clinic notes
- Share information with others

Learn how UHN protects your privacy.

Contact Us | Terms of Use | Privacy Policy | UHN.ca

Copyright© 2014 University Health Network

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab

COURAGE LIVES HERE

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab

COURAGE LIVES HERE

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

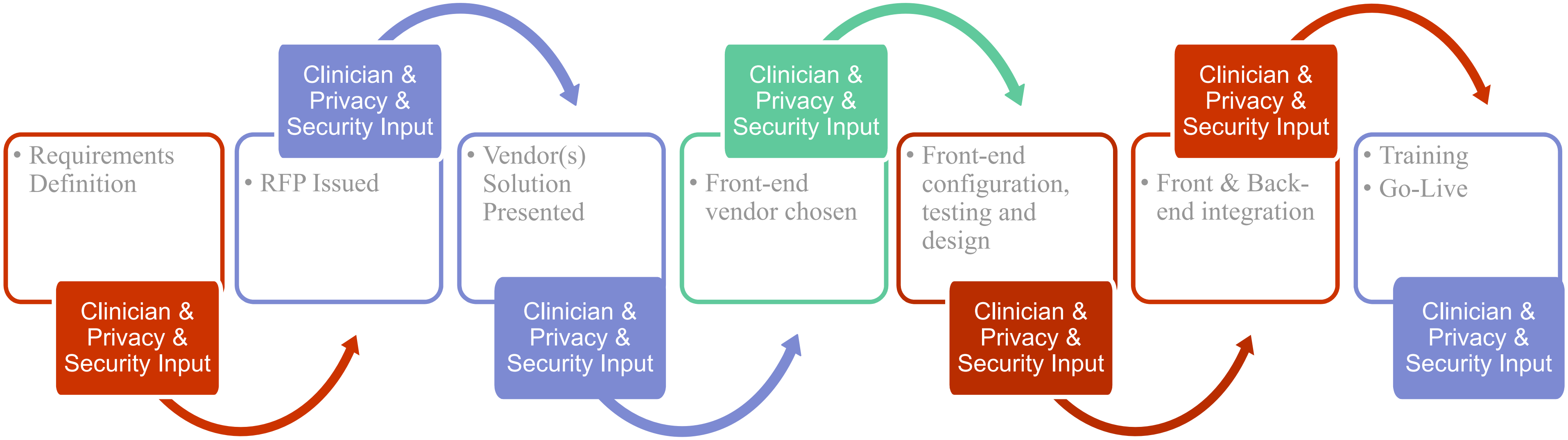
- **Proactive not Reactive – *Preventative not Remedial***
- **Privacy as the Default Setting**
- **Visibility & Transparency – *Keep it Open***

UHN
Toronto General
Toronto Western
Princess Margaret
Toronto Rehab
COURAGE LIVES HERE

Iterative Design Experience

Iterative Design Experience - ConnectingGTA

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



- Requirements Definition

Clinician & Privacy & Security Input

- RFP Issued

Clinician & Privacy & Security Input

- Vendor(s) Solution Presented

Clinician & Privacy & Security Input

- Front-end vendor chosen

Clinician & Privacy & Security Input

- Front-end configuration, testing and design

Clinician & Privacy & Security Input

- Front & Back-end integration

Clinician & Privacy & Security Input

- Training
- Go-Live

Clinician & Privacy & Security Input

Toronto General
Toronto Western
Princess Margaret
Toronto Rehab

COURAGE LIVES HERE

Privacy Engagement Options

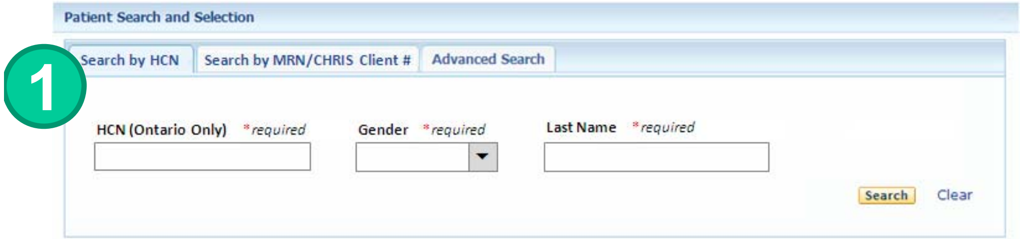
- Casual, automatic engagement – project team maturity
- Mapped against other similar systems (US and Canada)
  - E.g. terms of use, authentication & registration, proxys
- Environmental scan by students / contractors
  - E.g. Clarified patient desires and needs, identified need for culture change
- 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

Clinical/ Business Need	RFP	Technical Capability	PSWG	Final Functionality
Find the right patient. Find a patient with a unique # (OHIP or MRN) Find a patient in an emergency (no unique #)	Support searching with unique ID, MRN, OHIP, name, date of birth, gender	Possible: • different combinations of fields • some or all fields mandatory	✓ Include enough PHI for positive identification ✓ Use no more PHI than necessary ✓ Only return 1 patient whenever possible	Clinicians can do 1 of 3 searches: 1. OHIP & name & gender 2. MRN & org name 3. Advanced Search (any of name, DOB, gender, address) No information displayed if more than 5 results match

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab

COURAGE LIVES HERE



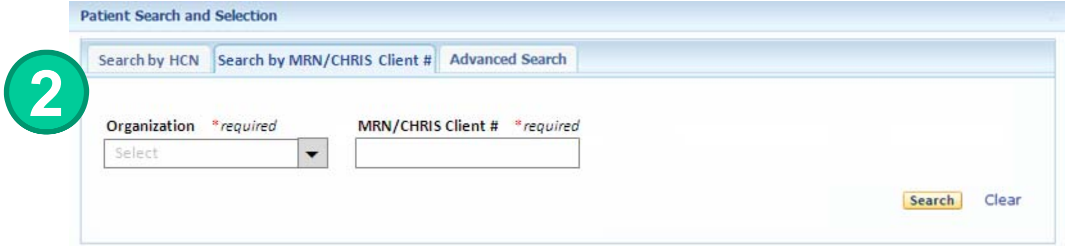
1

Patient Search and Selection

HCN (Ontario Only) *required

Gender *required

Last Name *required

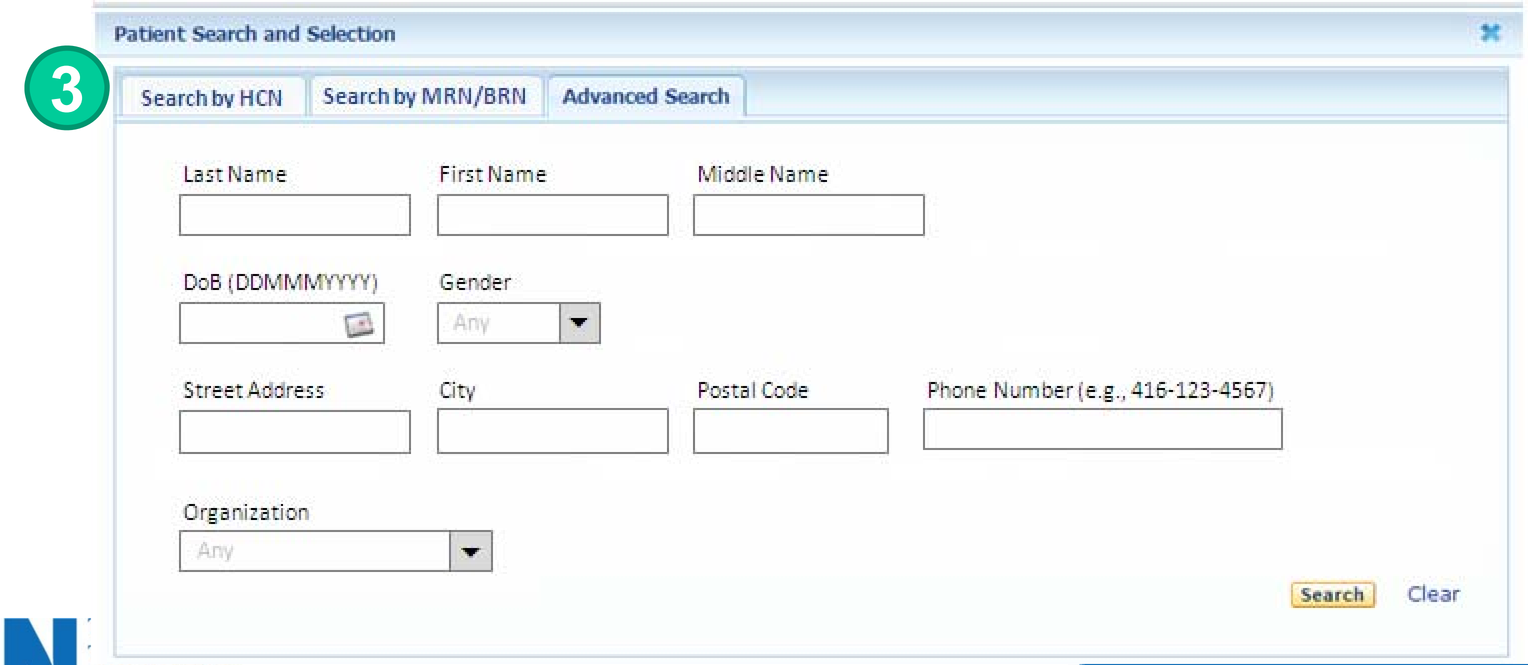


2

Patient Search and Selection

Organization *required: Select

MRN/CHRIS Client # *required



3

Patient Search and Selection

Last Name

First Name

Middle Name

DoB (DDMMMYYYY)

Gender: Any

Street Address

City

Postal Code

Phone Number (e.g., 416-123-4567)

Organization: Any

UHN
Princess Margaret
Toronto Rehab
COURAGE LIVES HERE

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

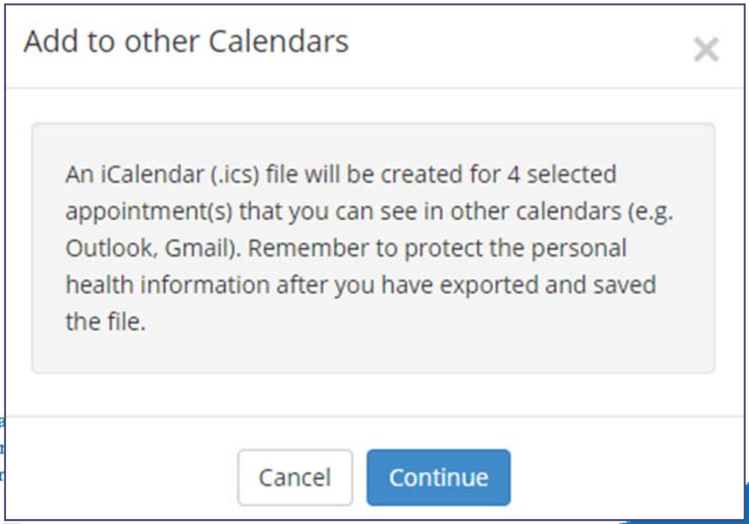
Full Functionality– ***Positive Sum, not Zero Sum***

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab

COURAGE LIVES HERE

Patient Portals – Downloading Appts

Patient Need	Privacy & Security	Clinical Consideration	Technical Capability	Patient Experience
Ability to download appointments to external calendars.	Patients must be informed of risks of downloading.	Reminder systems that do not require additional steps.	Appointment downloads include appointment details.	1. Patient consents to download 2. Patient selects appointments for download.



Add to other Calendars

An iCalendar (.ics) file will be created for 4 selected appointment(s) that you can see in other calendars (e.g. Outlook, Gmail). Remember to protect the personal health information after you have exported and saved the file.

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 <u>and</u> 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
416-340-4800 ext. 6620

Natalie Comeau, Supervisor, Privacy Advisory Services
Natalie.comeau@uhn.ca
647-539-4636