Sharing is Caring

Managing Privacy in Consumer Health Solutions

eHealth 2016 -- Vancouver, BC

120 Carlton Street, Suite 416
Toronto, Ontario, M5A 4K2
t. 416.642.2081
e. info@mdahealth.ca
w. www.mdahealth.ca

June 6, 2016

Consumer Health and Privacy

#eHealth2016

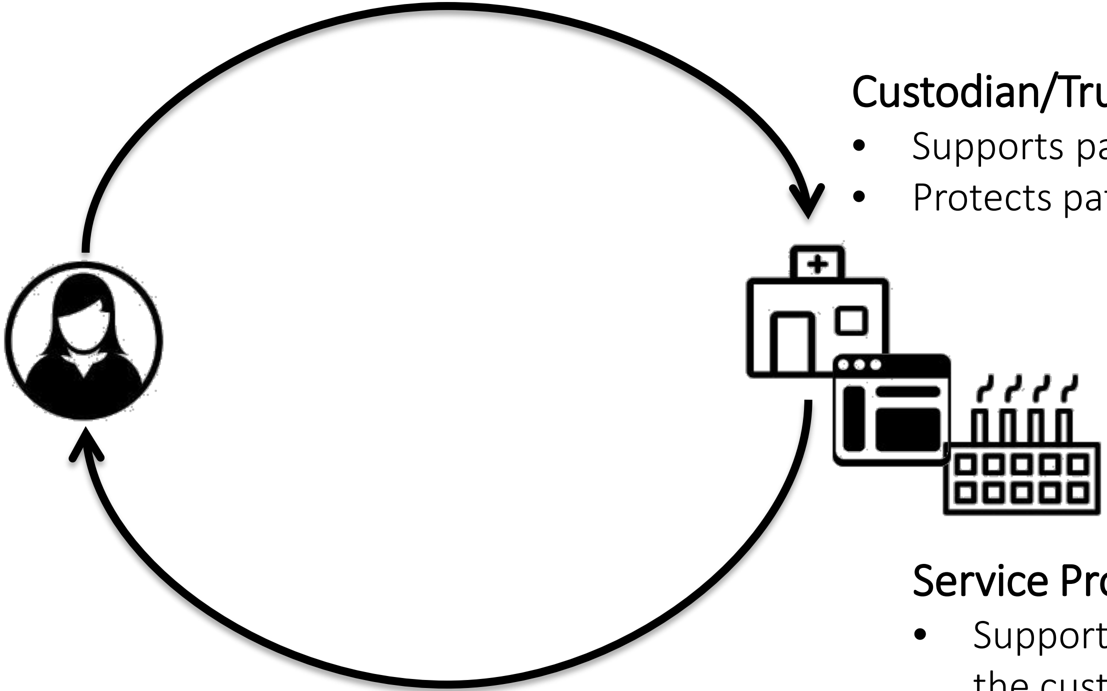
Introduction

How can healthcare providers enable access to patients’ information in the most privacy protective way?

- Quick introduction to privacy and consumer solutions
- Common privacy risks and considerations identified via privacy assessments
- Identifying the best safeguards to confidently enable access

Consumer Health and Privacy

Understanding privacy obligations will inform thinking on privacy risks and considerations



Patient

- Is entitled to access their own PHI
- Is informed of custodian’s privacy obligations

Custodian/Trustee/Steward

- Supports patient’s privacy rights
- Protects patient data

Service Provider

- Supports the obligations of the custodian
- Fulfills own obligations from agreements or legislation

Understanding Privacy and Patient Portals

Important things to keep in mind

- Patient portals don’t impose any new privacy obligations on providers
  - Another communications method for providers to collect and use patient data
  - Supports providers to meet patient access rights
  - Consent isn’t required to share patients’ data with them

- The key is how you fulfill your obligations in the context of the portal
  - Administrative and technical safeguards that will best protect the information

Key Privacy Risks and Considerations for Patient Portals

Learning from Privacy Impact Assessments conducted in the last five years

Privacy Risks

- Third party agreements and accountability mechanisms
- Account provisioning and identity management
- Patient education and awareness

Privacy Considerations

- Information release and data management strategy
- Meeting legislated privacy obligations for custodians/trustees/stewards

Risk 1: Account Provisioning and Identity Management

Registering patients and ensuring ongoing management of user accounts

Risks

- An account for a patient portal may be provided to the wrong person (intentionally or unintentionally)

- You need to ensure you confirm the identity of the patient or family members
- You need to ensure the patient has authorized family member access
- You need to bind the account to the identity, ideally in person (alternative is a code)
- You need a step to de-activate patient accounts when no longer needed

Risk 2: Service Provider Agreements and Accountability Mechanisms

Ensuring solution providers are supporting your capacity to meet your privacy obligations

Risks

- Service provider asserts control over the data that is in the custodianship of the provider
- Custodian doesn't impose appropriate obligations on the service provider to ensure support for custodian's obligations

- Carefully review privacy and security terms in agreements
    - to ensure accountabilities are properly characterized and obligations identified
    - to ensure that the service provider cannot use or disclose the information for any other purpose than to support the custodian
- Review service provider's privacy and security program to ensure alignment with obligations

Risk 3: Patient Education and Awareness

Ensuring patients understand their responsibilities when using the portal

Risks

- The patient doesn't understand where accountability for the information is transferred to them from the organization

- Ensure all account holders agree to a terms of use that covers appropriate use of the portal and describes the organization's safeguards
- Provide patients with information on how to best safeguard their information
  - Not sharing account information
  - Securely accessing information (e.g., in public places)
- Where the patient is providing information via the portal, inform them that this information is now in the custody of the org

Consideration: Information Release and Data Management Strategy

Deciding the business rules governing the release of patient information

- Done at the planning stages for a portal but revisited periodically
- Consider your objectives for the release of patient information, as well as your rights and obligations
  - Information you may not wish to share due to its sensitivity or due to the context required for the patient to understand it
  - The timing and processes for the release of information (e.g., time delay for releasing test results to enable provider contact)
- Note that information not released through a portal is still accessible to patient through access requests or other care delivery channels

Consideration: Meeting your core privacy obligations

- Define your approach for extending the way you meet your core privacy obligations to support delivery of the portal
  - Access and corrections
  - Logging and audit
  - Breach management
  - Inquiries and complaints
  - Consent directive management where applicable

Going Forward

Takeaways for organizations considering implementing patient portals

- Extend your business processes and strategies for management of personal health information to include release of patient information via the portal
- Consider the patient’s experience of using the portal and accessing their health information. How can you best support them to manage their PHI in a privacy protective way?
- Carefully review service provider agreements and establish clear understanding of shared processes for meeting your privacy obligations

Thank you!

See also: COACH's *Privacy and Security for Patient Portals: 2012 Guidelines for the Protection of Health Information*

Connect with me

416.642.2081 x229

darcelle@mdahealth.ca

linkedin.com/in/darcellehall

@mdahealth