Granular Data Segmentation to Protect Privacy and Promote Equitable Interoperability

Hannah K. Galvin, MD, FAAP, FAMIA
Chief Medical Information Officer, Cambridge Health Alliance
Assistant Professor of Medicine, Tufts University School of Medicine
Co-Founder and Co-Chair, Protecting Privacy to Promote Interoperability (PP2PI) Workgroup
I have no conflicts to disclose.
Protecting Privacy to Promote Interoperability Workgroup

- Formed in 2018, formalized in 2020
- Supported by HIMSS, IHE USA and The Drummond Group
- Multidisciplinary workgroup of > 160 industry experts
Stakeholders across the U.S. healthcare ecosystem

- Healthcare Provider Organizations/Institutions
- Professional Societies
- Standards Development Organizations
- Health IT Vendors
- Health Information Exchanges
- Interoperability Frameworks
- Payers
- Government
- Government and Non-Government Contractors
- Privacy Law and Ethics Experts
- Patient Advocates
Paul

- 72 y/o Retired Teacher
- Presents for Annual Physical
- History of alcoholism, relapses over past decade since son killed in Afghanistan; underlying depression diagnosed – improving with medication (SSRI) and counseling

Problem list: Hypertension, atrial fibrillation, gout, s/p transient ischemic attacks x 3 in past 2 years.
Donna, Paul’s Wife

- 74 year old retired Accountant
- Designated as his healthcare power of attorney (in waiting)
- States Paul has had difficulty with short term memory, including medical appointments.

Requests proxy access to Portal account (including OpenNotes)
Examining Paul Alone

- States he has not discussed his relapses or depression diagnosis with Donna
- Admits it would be helpful for her to have access to his basic medical info including INR appointments
- Expresses desire for optometrist to not have access to mental health/Substance use disorder information

Expresses resentment that Donna would “pry” into his medical affairs “It’s none of her business.”
Juliana

- 16 y/o F with PMH of asthma presents for WCC.
- Sexually active with 1 male partner, using condoms “most of the time.”
- No genitourinary complaints; requests Rx for OCP.
- Wants to keep all reproductive health issues confidential from parents.
You discuss contraception options.

Send OCP Rx and urine GC/CT.

Next day: results return with +CT, neg GC.

You call Juliana on cell with results and plan.

Send in Rx for azithro to her local pharmacy and EPT for her boyfriend.

Tie Rx to ICD-10 dx A74.9 (CT) and add it to problem list.
Juliana

- Juliana has full access to her patient Portal.
- Juliana’s parents also have access to her Portal as proxies. Typically use Portal to refill her asthma meds and for reminders of her Allergy appts.
  - Med and Problem lists available (curated view of EHR).
  - Results previously auto-released in 5-days, soon to be released immediately per 21st Century Cures.
  - OpenNotes also available per 21st Century Cures.
- EOB for lab test and Rx sent to parents (guarantors).
Framing the Larger Problem

Sharing of private health care information between providers, organizations, patients, & families can only be freely accomplished when there is agreement on:

- Need for patient safety
- Need for privacy

How to:
- Identify
- Tag
- Protect
- Display
- Share/re-share

Sensitive data
Relevant Laws

- Federal
  - Constitutional Law
  - HIPAA
  - 42 CFR Part 2
  - Adolescents: Title X & FERPA

- State

- International
  - GDPR
What Areas of the Chart May be “Sensitive”?  

- **Registration/demographic data**  
  - Sexual orientation/gender identity  
  - Consent to treat for sensitive procedure  

- **Patient-level data**  
  - Problem list, PMH, PSH, FHx  
  - Meds, allergies  
  - Social Hx, SDoH  

- **Episode-level data**  
  - Visit note, individual sections of note  
  - Procedure documentation  
  - Screening questionnaire  
  - Diagnostic tests and results
What Types of Data do these Encompass?

- **Registration/demographic data**
  - Sexual orientation/gender identity – vendor-specific structured
  - Consent to treat for sensitive procedure – .pdf

- **Patient-level data**
  - Problem list, PMH, PSH, FHx – SNOMED, ICD-10
  - Meds, allergies – RxNorm
  - Social Hx, SDoH – vendor-specific structured, unstructured

- **Episode-level data**
  - Visit note, individual sections of a note – unstructured
  - Procedure documentation – unstructured, .pdf, image files
  - Screening questionnaire – .pdf, vendor-specific structured
  - Diagnostic tests and results – LOINC, others
Where Does the Data Go?

- Ancillary services
- Other providers/health care organizations
- Patient portal
- Printed reports
- 3rd-party apps
- HIE’s
- DPH
- ACO’s/CIN’s (Quality, P4P)
- Payors → EOB
How is Data Access Controlled?

*Not all systems have the same defined roles or roles defined in the same way*
Why is this such a challenge?

- Many different stakeholders
- Many different types/flows of data (both internal and external)
- Questions of data ownership
- Access control definitions
- Questions of patient safety vs. right to individual privacy
- Development/implementation of standards complex

Industry: “Too big to tackle”
Many organizations enable blunt privacy protections to comply with state laws

- Patients must choose to share ALL or NONE of their data
  (May be done algorithmically)
- Concern for “data blocking”
- May be inadvertently producing healthcare disparities
Who is affected?

Who has potentially sensitive data?

• >1.2 million people with HIV at end of 2018\(^1\)
• 1 in 5 people in the US with a sexually transmitted infection (STI) in 2018\(^2\)
• 1 in 5 US adults (51.5 million) with a mental illness in 2019\(^3\)
• 1 in 13 US adults (19.3 million) had a substance use disorder (SUD) in 2019\(^4\)
• 1 in 5 women & 1 in 14 men reported sexual violence in their lifetime (2015).
• 1 in 4 women & 1 in 10 men reported intimate partner violence in their lifetime (2015).\(^5\)

• “Sensitive” may mean different things to different people.

\(^1\) [http://www.cdc.gov/hiv/statistics/basics/ataglance.html](http://www.cdc.gov/hiv/statistics/basics/ataglance.html)
\(^5\) [https://www.cdc.gov/violenceprevention/datasources/nisvs/summaryreports.html](https://www.cdc.gov/violenceprevention/datasources/nisvs/summaryreports.html)
Medical Mistrust

Higher in historically disenfranchised populations. Associated with decreased compliance with health care recommendations.

• African American men w/ prostate cancer with lower levels of trust in health care system & providers vs. white men

• African American women with FHx of breast CA less likely to get recommended BRCA testing; in sample of 100, associated with medical mistrust.

• Black MSM’s report:
  • Experiencing racial & sexual orientation stigma from providers (29%)
  • Mistrust of medical establishments (48%)
  • ↑Stigma/mistrust associated with ↑gap since last exam/HIV care.

Medical Mistrust: Hypothesis

Providing enhanced privacy choices to populations with high levels of medical mistrust will:

↑ Trust in health care establishment

↑ Adherence to care recommendations

↑ Health of populations
What about DS4P?

• Data Segmentation for Privacy (DS4P): original standard allowed tagging of C-CDA metadata (document, section, or entry level) indicating data contained therein is restricted and subject to restrictions on redisclosure.

• 2 Criteria: Send and Receive.

• Successfully piloted by VA/SAMHSA, NETSHARE, Cerner.

• HL7 v 2.9 and FHIR IG’s developed
  • FHIR IG allows for granular security labeling

• Proposed/adopted by HHS/ONC:
  • Optional certification MU3
  • 21st Century Cures: optional pedi certification/OUD prevention & tx
The Patient receives care at their **local hospital** for a variety of conditions, including substance abuse as part of an Alcohol/Drug Abuse Treatment Program (ADATP).

Data requiring additional protection and consent directive are captured and recorded. The patient is advised that the protected information will not be shared without their consent.

A clinical workflow event triggers additional data to be sent to Provider/Organization 2. This disclosure has been authorized by the patient, so the data requiring heightened protection is sent along with a prohibition on redisclosure.

Provider/ Organization 2 electronically receives and incorporates patient additionally protected data, data annotations, and prohibition on redisclosure.

*Content courtesy of Johnathan Coleman, CISSP – DS4P Initiative Coordinator, S&I Framework, OCPO/OST/ONC/HHS (CTR)*
Consent2Share (C2S): open source tool developed by SAMHSA utilizing FHIR consent resource to provide consent management for data tagged using DS4P. Allows patients to make meaningful choices about how to share their sensitive data.

- Patient consent management (PCM): front-end, patient facing user interface; allows patients to define their privacy policy and provide informed consent.
Consent2Share (C2S): open source tool developed by SAMHSA utilizing FHIR consent resource to provide consent management for data tagged using DS4P. Allows patients to make meaningful choices about how to share their sensitive data.

- Access Control Services (ACS): back-end control system to integrate with EHR’s and HIE’s; provides privacy policy configuration, management, decision making, and policy enforcement.
Previous Efforts Lagged

- Data Segmentation for Privacy (DS4P) and Consent 2 Share (C2S) adoption has lagged due to:
  - Inability to meet many high-priority clinical use cases
  - Implementation not easily scalable across organizations
  - Issues related to patient safety and usability not adequately addressed by pilots
  - Lack of financial or regulatory stimulus
How we are approaching things differently?

1. Building off of previous work
2. Expanding scope of use cases to more widely encountered situations
3. Cross-industry stakeholder representation
4. Focus on consensus-driven implementation guide as a key deliverable
5. Leveraging advances in technologies such as NLP
Workgroup Deliverables and Status

- Develop set of nationally-acceptable use cases
  - Adolescent/reproductive health
  - Geriatric/mental health
  - Adult Social Determinants of Health
  - Maternal/baby

- Draft minimal set of potentially-sensitive data elements

- Standards gap analysis and revision

- Develop consensus-driven guidance
  - Terminology value sets
  - Recommendations for role-based vs. user-based security
  - Visualization of redacted data
  - Utilization of redacted data in decision support
  - Policies/procedures for break-the-glass access to data
Workgroup Structure

Foundational sub-groups
- Clinical
- Usability
- Implementation
- Standards & Terminology

Overarching sub-groups
- Patient perspective
- Legal & Policy
- Ethics
Progress Pre-2021

May 2020
Launched PP2PI WG

June
- Developed consensus around the WG charter as well as establish logistics.

July
- Proposal of WG guiding principles and use cases

August
- Proposal for sub-groups and organization to move towards WG deliverables
- Create sub-groups, identify chairs, and subgroup output

September
- Sub-group charter and first meetings

October
- Sub-group charter and first meetings
- Early subgroup deliverables

December
- Progress towards clinical use cases and other subgroup charters
### PP2PI Roadmap

**Use cases developed**
2020-Q1 2021

- Clinical team has developed 4 initial use cases

**Final SDoH use case**
Q2-3 2021

- Finalize SDoH use case with feedback from Gravity Project

**Hone use cases**
Q3-4 2021

- Adjust use cases as needed based on feedback from other subgroups

**Sensitive data elements**
Q3-4 2021

- S&T builds profile with sensitive data element story around each use case

**Terminology value sets**
2021-2022

- Identify/update terminology value set to fit use cases

**Standards revision**
2022-2023

- S&T work with HL7 Security WG to ballot for standards revision, starting w/ 1 use case

**Persona pieces**
Q3-4 2021

- U&I turn use cases into persona usability pieces and storyboard these

**Implementation Questions**
Q3-4 2021

- Develop questions and process for Delphi Method v 1.0

**Prototype Implementation**
2022-2023

- Build basic prototypes to advance work towards sandbox-MVP
PP2PI Roadmap

Use cases

Standards & terminology

Consensus on Implementation Guidance via Delphi Methodology

Sandbox demonstration

Implementation guide

Real-world demonstration

2022

2023

2024
How to Get Involved

For more information or get involved, please see our website and fill out our interest form at:
https://www.drummondgroup.com/pp2pi/

Or contact:
serena.mack@drummondgroup.com
hagalvin@challiance.org