Privacy in HIE and Patient Matching - Too little or Too much?

Adrian Gropper, MD
CTO, Patient Privacy Rights
January 30, 2020

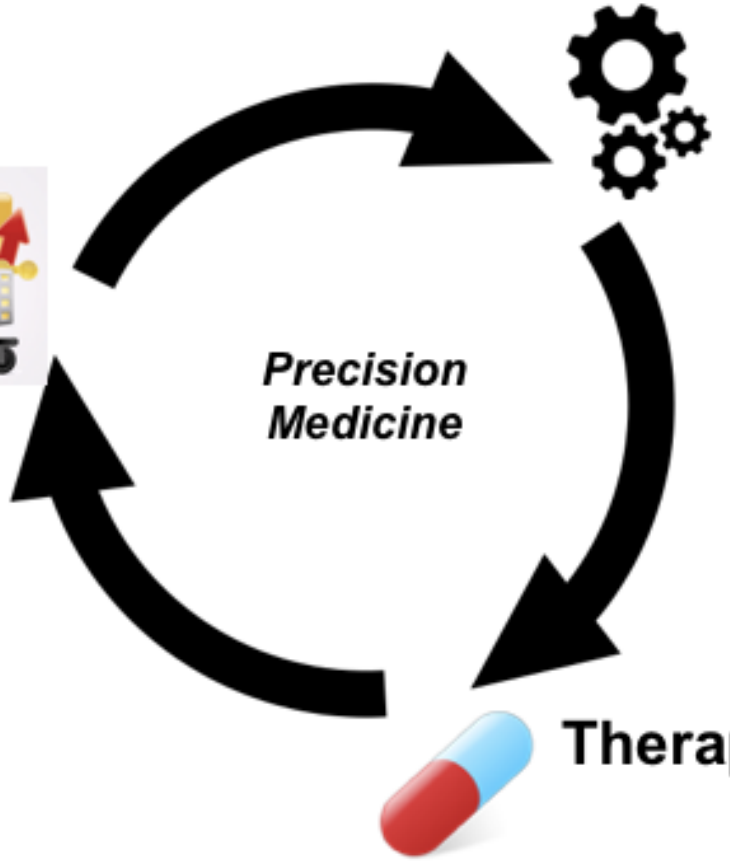
patientprivacyrights

Me:

1. Mechanical / computer engineer
2. Physician (non-practicing)
3. Medical device developer
4. **Career: Medical device entrepreneur**
5. Chemistry analyzers
6. Radiology systems
7. Telemedicine
8. Health records
9. Privacy expert in standards workgroups
10. **Current: Patient-centered health records developer and advocate**

You

- Physician notes
- Insurance
- Imaging
- Labs
- Diet
- Exercise
- Genomes
- other ‘omes
- Prescriptions
- Social Media
- Subsidies
- Family history
- ...



Decision Support

- Physicians
- Internet
- Research
- Costs
- AI
- Directories
- Reputation

Brief HIE tutorial for clinicians and administrators

- 2002: HIPAA and consent
- 2004: NHIN
- Dueling access principles - with or without consent
- Dueling interoperability principles - documents or APIs
- Health Information Exchange essentials
- 2019: TEFCA
- 2020: Issues
- Apps and regulations
- Decentralization alternative: HIE of One Trustee

… Part 2: Patient Matching and other privacy perspectives

2002 Amended HIPAA Privacy Rule

67 Fed. Reg. 53,183

"The consent provisions…are replaced with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, and healthcare operations."

Result: 2M+ US health data holders treat our data as corporate assets

What is the NHIN?

Nationwide Health Information Network

PROCESS. METHODOLOGY. SPECIFICATIONS. POLICY. GOVERNANCE. TECHNOLOGY.

The Nationwide Health Information Network (NHIN), a program under the Office of the National Coordinator for Health Information Technology (ONC), was established in 2004 to improve the quality and efficiency of healthcare by establishing a mechanism for nationwide health information exchange. The NHIN is a set of conventions that provide the foundation for the secure exchange of health information that supports meaningful use. The foundation includes technical, policy, data use and service level agreements and other requirements that enable data exchange, whether between two different organizations across the street or across the country.

Participants in the NHIN agree to support a common set of web services and data content (NHIN Core Services) that enables private, secure and interoperable communication of health information among NHIN participants across the public Internet.

A critical component of the NHIN is the trust model that bridges a diverse group of public and private entities. This trust model provides a common foundation for privacy and security obligations, accountability and governance in the midst of varying diverse federal, state and local policies and laws. One of the

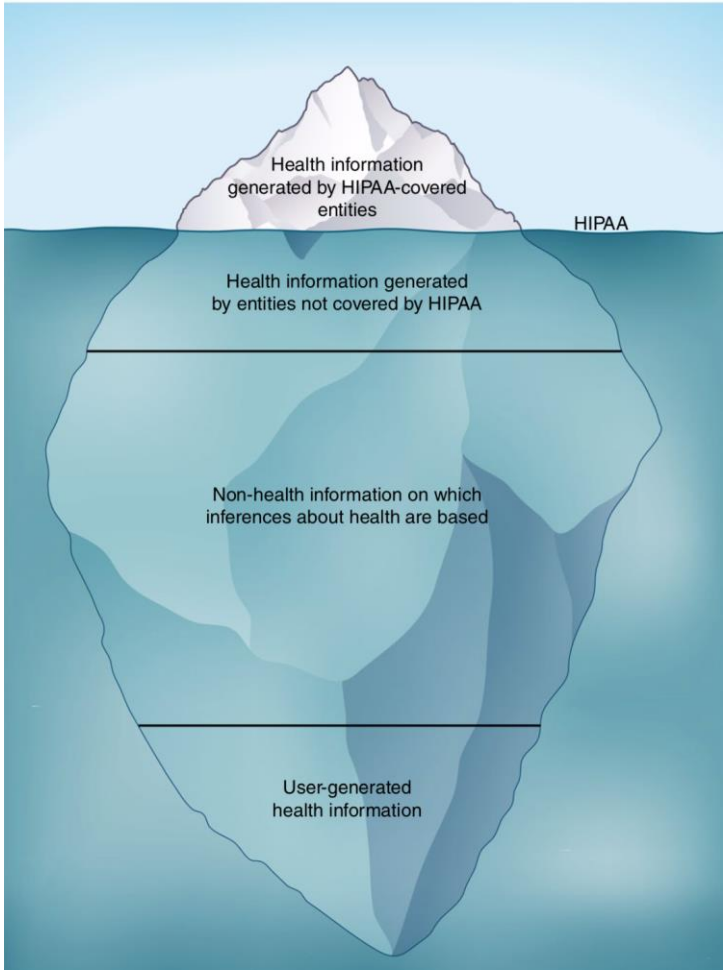


Image From: Privacy in the age of medical big data

Access Principle

HIPAA T/P/O ● Treatment ● Payment ● Operations	**Patient-Directed** ● Fax ● US Mail ● Digital
No Consent	Needs Specific Destination
No Transparency	No Surprises
Opt-out	Opt-in
Patient Matching	Patient Engagement
Limited Scope	Universal (including behavioral and SDOH)
Future: ● TEFCA? ● Epic Everywhere?	Future: ● Apple? ● Apps ● Standards (HIE of One)

Interoperability Technology Alternatives

Document

- Example: fax, email, Direct
- Pushed
- Sender decides
- Cheap to send
- Expensive to process on receipt
- Easy to sign / authenticate
- Intermediaries are irrelevant

API

Application Programming Interface

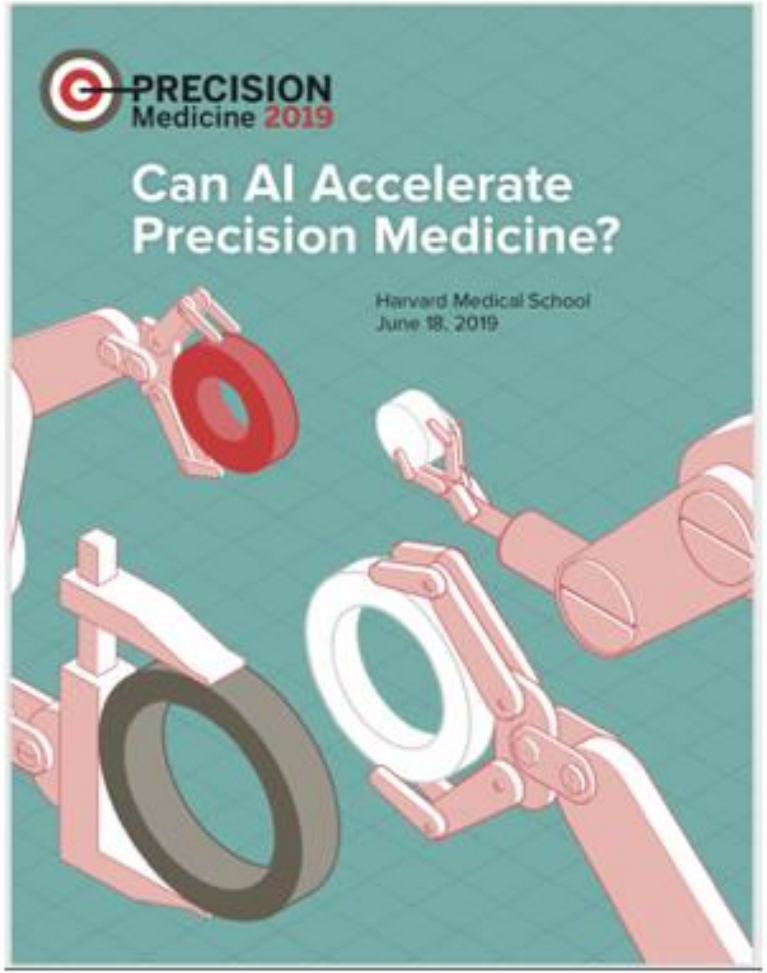
- Example: Web, Expedia, Netflix
- Pulled
- Recipient decides
- Cheap to send
- **Easier to process on receipt**
- Hard to sign / authenticate
- **Intermediaries are a problem**

HIE Essentials

- Access Governance
- Directories
- Messaging
- Standards
- Patient Matching
- Record / Encounter Locator
- Sustainability

HIE Options

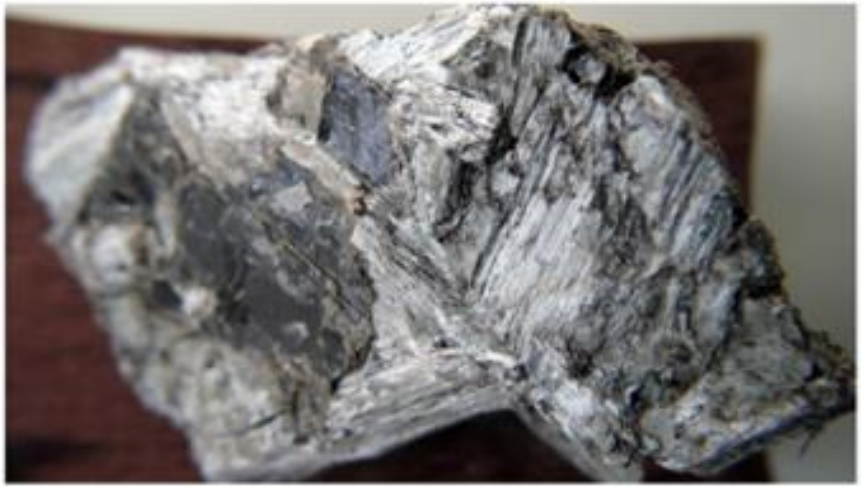
- Registry Filings
- Health Records
- Analytics
- Patient Access



HEALTH TECH

What if AI in health care is the next asbestos?

By CASEY ROSS @caseyrross / JUNE 19, 2019



A sample of asbestos
RICK BOWMER/AP

BOSTON — Artificial intelligence is often hailed as a great catalyst of medical innovation, a way to find cures to diseases that have confounded doctors and make health care more efficient, personalized, and accessible.

But what if it turns out to be poison?

TEFCA

The Office of the National Coordinator for Health Information Technology

The Trusted Exchange Framework and Common Agreement Draft 2

April 23, 2019

This informational resource describes select proposals in the TEFCA but is not an official statement of any policy.
Please refer to the official version of the TEFCA

Goals

Provide a single "on-ramp" to nationwide connectivity

Electronic Health Information (EHI) securely follows you when and where it is needed

Support nationwide scalability

Exchange Modalities

QHIN Broadcast Query

A QHIN's electronic request for a patient's EHI from all QHINs.

QHIN Targeted Query

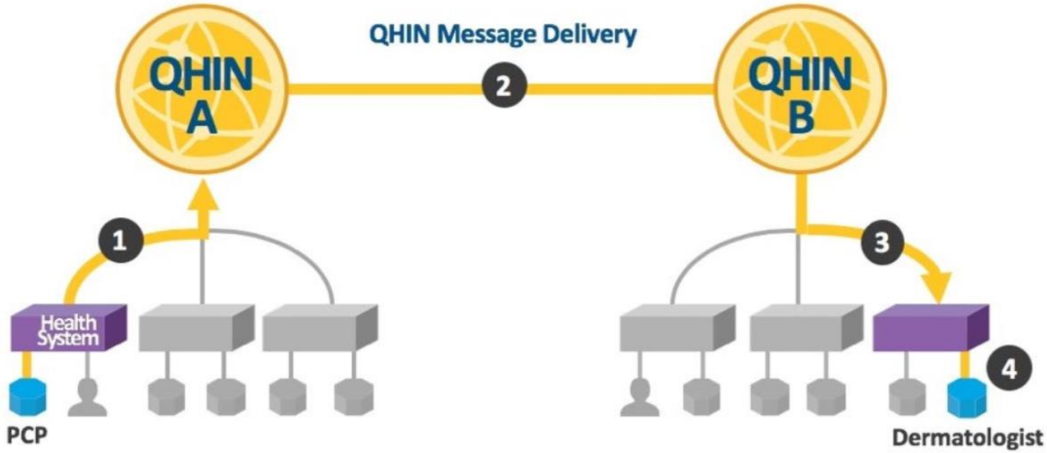
A QHIN's electronic request for a patient's EHI from specific QHINs.

QHIN Message Delivery (Push)

The electronic action of a QHIN to deliver a patient's EHI to one or more specific QHINs.

Exchange Purpose Example

Treatment*

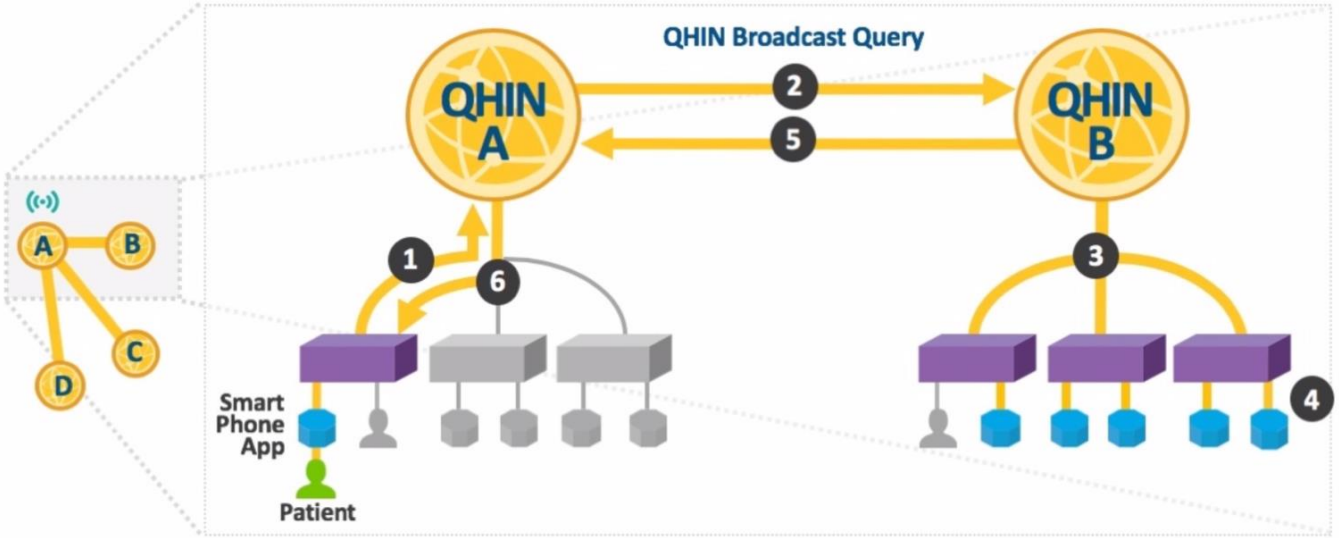


1. Primary Care Provider (PCP) (Participant Member) refers patient to Dermatologist, and sends care summary to QHIN A for Treatment
2. QHIN A initiates QHIN Message Delivery to send care summary to the appropriate QHIN B
3. QHIN B sends care summary to the appropriate Participant
4. Participant delivers care summary to the Dermatologist (Participant Member)

**Only applies to HIPAA covered entities and business associates* 39

Exchange Purpose Example

Individual Access Services



1. Patient (Individual User) uses a smart phone app (Participant Member) to make a medical records request via the Participant to the QHIN for Individual Access Services
2. QHIN A initiates QHIN Broadcast Query to all connected QHINs
3. QHINs B, C, D execute their query methodology to request medical records from all appropriate Participants and their Participant Members
4. Participant Members and Participants respond with medical records
5. QHINs B, C, D send medical records to QHIN A
6. QHIN A sends medical records to Participant, who sends to smart phone app (Participant Member), who sends to Patient (Individual User)

Structure of a Qualified Health Information Network

A **QHIN** is an entity with the technical capabilities to connect health information networks on a nationwide scale.

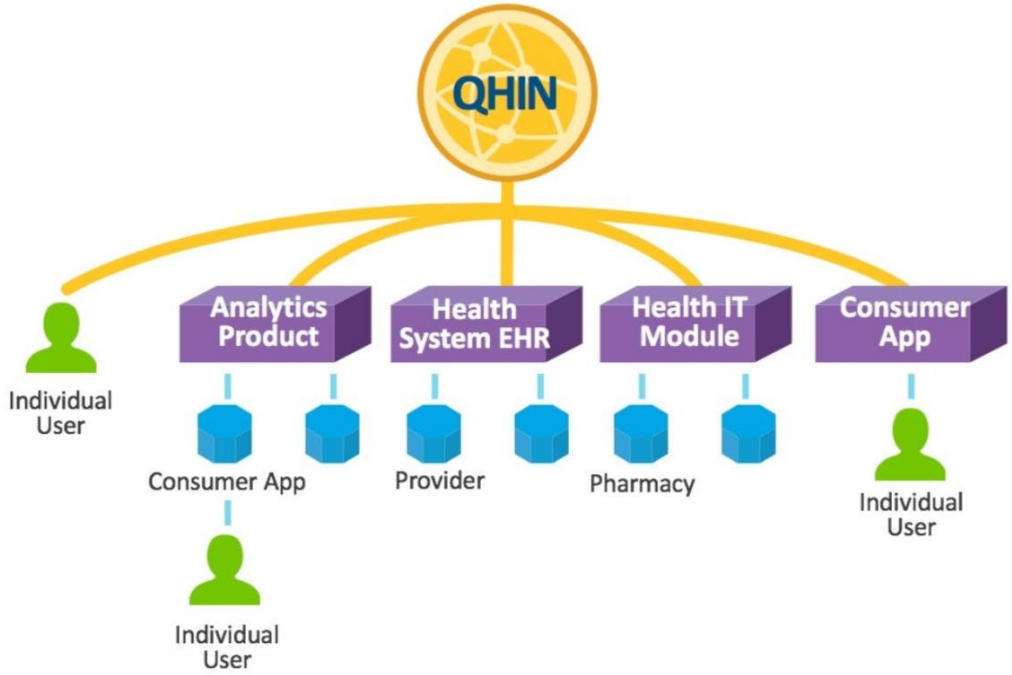
Participant
A natural person or entity that has entered into a Participant-QHIN Agreement to participate in a QHIN.

Participant Member
A natural person or entity that has entered into a Participant Member Agreement to use the services of a Participant to send and/or receive EHI.

Individual User
An Individual who exercises their right to Individual Access Services using the services of a QHIN, a Participant, or a Participant Member.

QHIN Example: Network of Health IT Developers

In this example, the QHIN supports a broad range of different health IT developer Participants. The users of the health IT developers' products are Participant Members. Individual Users connect directly to the QHIN, Participants, and Participant Members.



Issues with TEFCA and institutional HIE

- Centralized governance
- Security
- Complexity
- Enforcement
- Consent management
- Patient matching
- Innovation
- Cost and sustainability
- Scope of data under surveillance

… versus a decentralized alternative

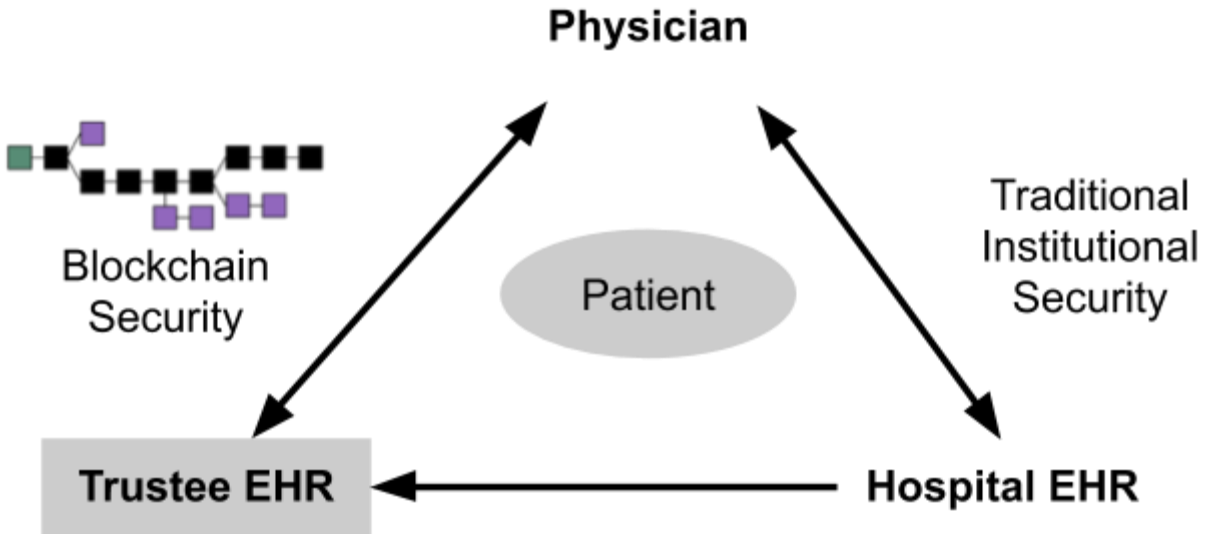
Apps, Digital Health, SDOH, PRO, AI... oh my!

- The “Goldilocks Dilemma”
- Forbidden knowledge
- “Code of Conduct”
- App ratings
- How intrusive are the Social Determinants of Health?
- Who captures and judges the Patient Reported Outcomes?
- How do we regulate AI?

Do FQHCs have a unique role?

Who decides?
Who decides who decides?

Decentralized, Patient Centered Alternative



http://bit.ly/TrusteeWhitePaper

End of part 1

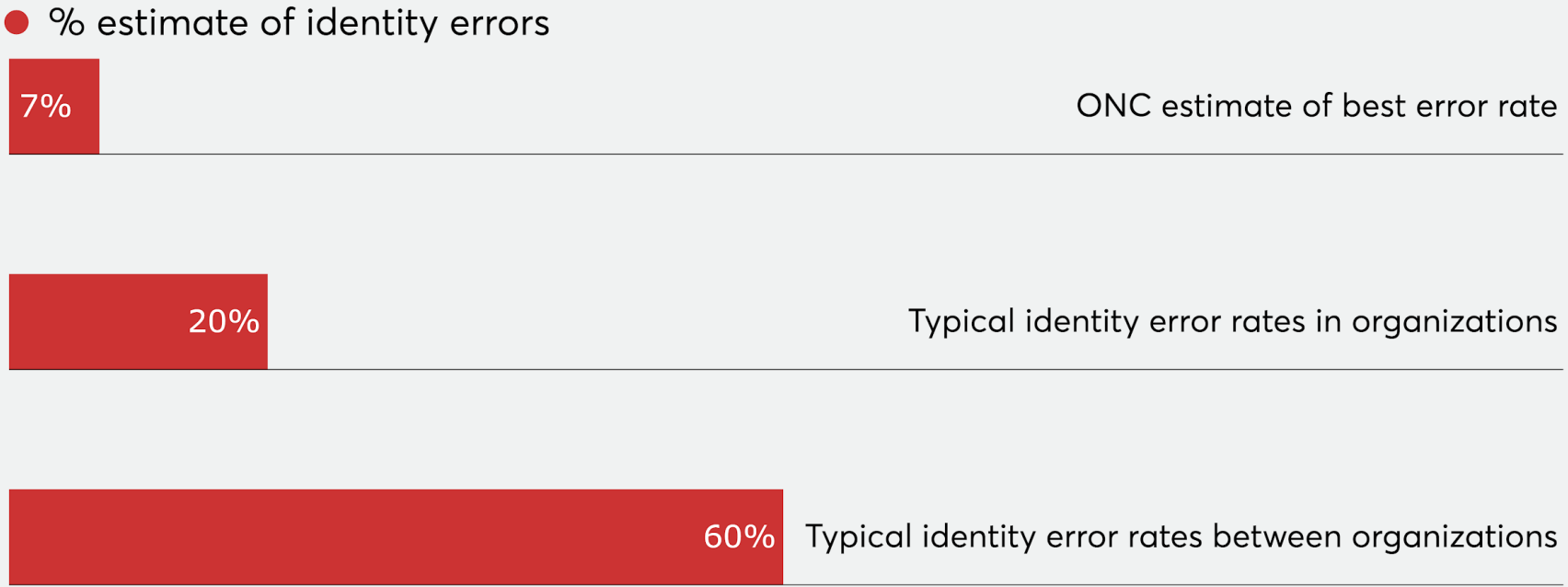
Questions?

Part 2: Patient Matching and other privacy issues

Agenda

- Three approaches to identity
  - Patient Matching
  - National Patient Identifier
  - Digital or Self-Sovereign Identity
- Patient matching = Surveillance
- Unique National Patient ID
- Biometrics
- Self-sovereign Digital ID

Identity matching issues remain a problem



Source: ONC, CHIME

HIT Think What the House's decision to lift the ban on funding NPI means

By Jerris Heaton

January 02, 2020, 3:45 p.m. EST

" Essentially, an NPI system would assign each U.S. citizen a unique number to identify them across the healthcare system, a move that had been previously tabled for more than two decades due to privacy concerns.

In theory, such a system will help prevent duplicate patient records, make the transfer of patient information simpler and ease other unnecessary costs associated with patient identification."

https://youtu.be/H69l_trRArU

Patient Matching

- Matches HIPAA - no consent
- Benefit: No patient engagement
- Surveillance
  - Scope. How much surveillance?
  - What is success?
- Privacy
  - Referential matching
  - Who knows all?
  - Social determinants?
  - Behavioral health?
- What will TEFCA do?

Surveillance-based Identity Examples

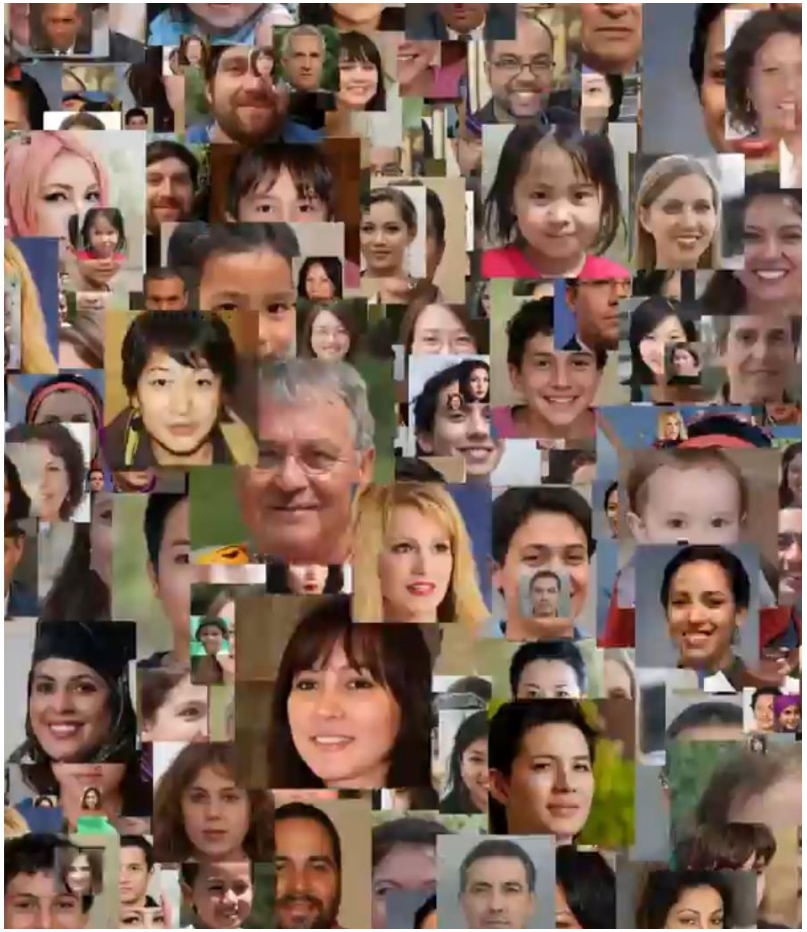
- Facial recognition
- Schools
- Smart Cities
- Location
- Media - News, Entertainment
- Social Media
- Purchasing
- Credit
- Health Care?

The New York Times

Account

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and "might lead to a dystopian future or something," a backer says.



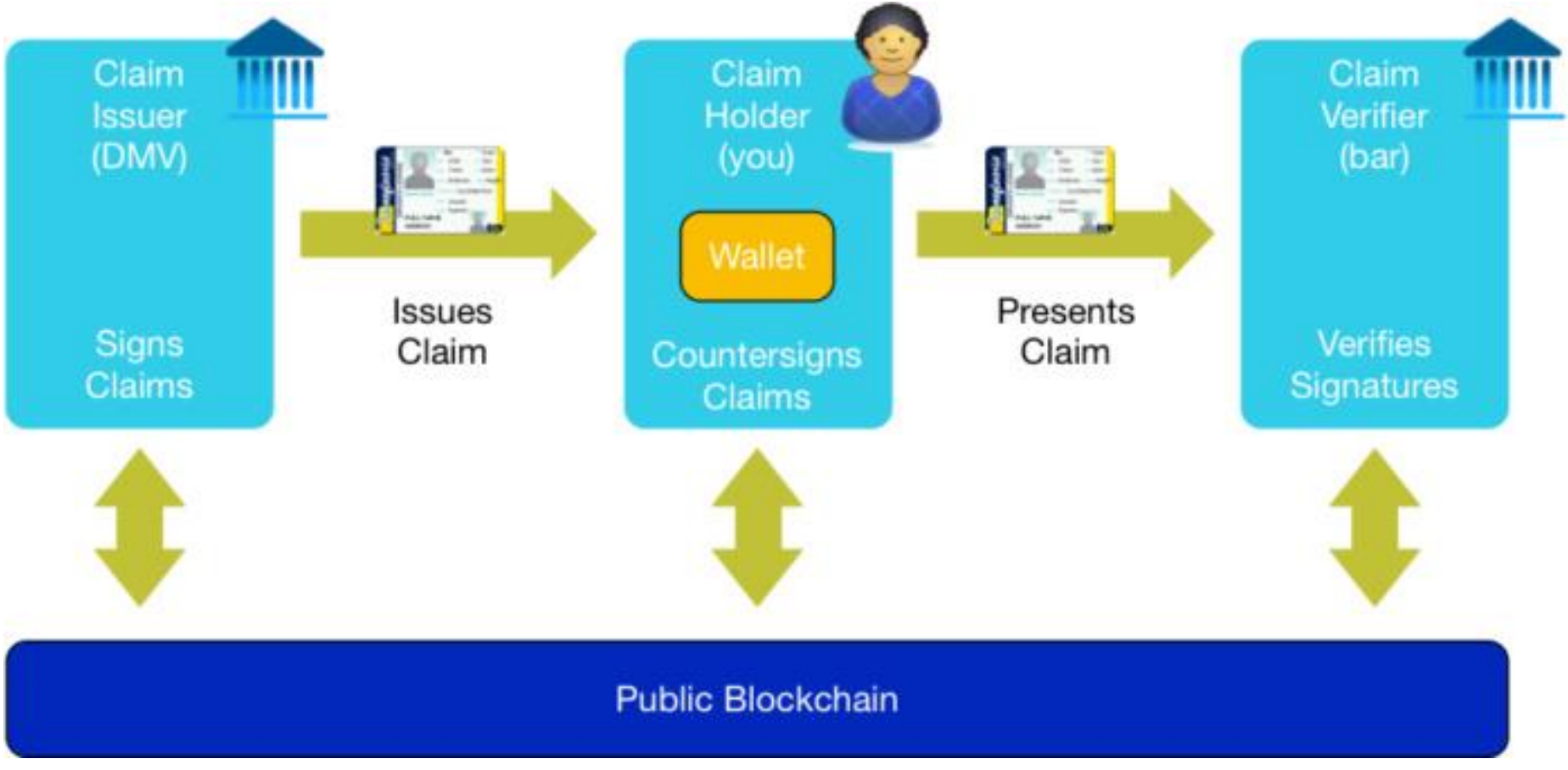
Unique IDs

- Coerced
  - Driver’s License
  - Passport
  - SSN
  - Medicare ID
  - Iris
- Voluntary
  - Email
  - Cell Phone
- Hybrid
  - Bank Account
  - Insurance Account

Biometrics

- Local vs. Centralized
- Proprietary
- Expensive
- Supervised
- Examples
  - Face
  - Gait
  - Iris
  - Fingerprint
  - Palm
  - DNA
  - Immune Cells
- Many security and privacy issues
- Combinations

Self-Sovereign Identity



Self-Sovereign Identity

- Decentralized
- Privacy preserving
- Blockchain technology
- Self-verifying
- No more passwords
- Digital signatures
- Requires Tech
  - Smartphone
  - Smart Card
  - Token
- Public and private sector
- New

Complexity and Confusion

- Patient matching is the incumbent
- Standards and Unique IDs will improve patient matching
- Is patient matching good enough for TEFCA?
- The role of biometrics is unclear
- Digital identity is the future, but when?
- Will artificial intelligence change the game?
- Can we have a (precision medicine) future without consent?

How much patient engagement?

nature medicine
FOCUS | REVIEW ARTICLE
https://doi.org/10.1038/s41591-018-0272-7

Privacy in the age of medical big data

W. Nicholson Price II[1,2,3] and I. Glenn Cohen[2,3,4]*

Big data has become the ubiquitous watch word of medical innovation. The rapid development of machine-learning techniques and artificial intelligence in particular has promised to revolutionize medical practice from the allocation of resources to the diagnosis of complex diseases. But with big data comes big risks and challenges, among them significant questions about patient privacy. Here, we outline the legal and ethical challenges big data brings to patient privacy. We discuss, among other topics, how best to conceive of health privacy; the importance of equity, consent, and patient governance in data collection; discrimination in data uses; and how to handle data breaches. We close by sketching possible ways forward for the regulatory system.

Thank you!

agropper@patientprivacyrights.org

patientprivacyrights