Federated Learning to Collect Mobile Patient-Reported Outcomes

Dr. Sara Jordan

Dr. Rachele Hendricks-Sturrup

Future of Privacy Forum

Washington DC, USA

November 12, 2020

worldusability**day**

Certified Section 508 Compliant

Human-Centered Design
Center of Excellence

ABOUT THE FUTURE OF PRIVACY FORUM

The Supporters

150+
Companies

25+
Leading
Academics

15+
Advocates and
Civil Society

5
Foundations

The Mission

Bridging the policymaker-industry-academic gap in privacy policy
Developing privacy protections, ethical norms, & responsible business practices

The Workstreams

Connected Cars
Student Data

Location & Ad Tech
Internet of Things
Health & Genetics

Ethics & De-identification
Smart Cities

Our goal is to <u>identify, codify, and champion</u> the structures and commitments needed to support the generation, exchange, and use of sensitive data (both regulated and unregulated) for individual, private, and public purposes in a trusted and ethical manner.

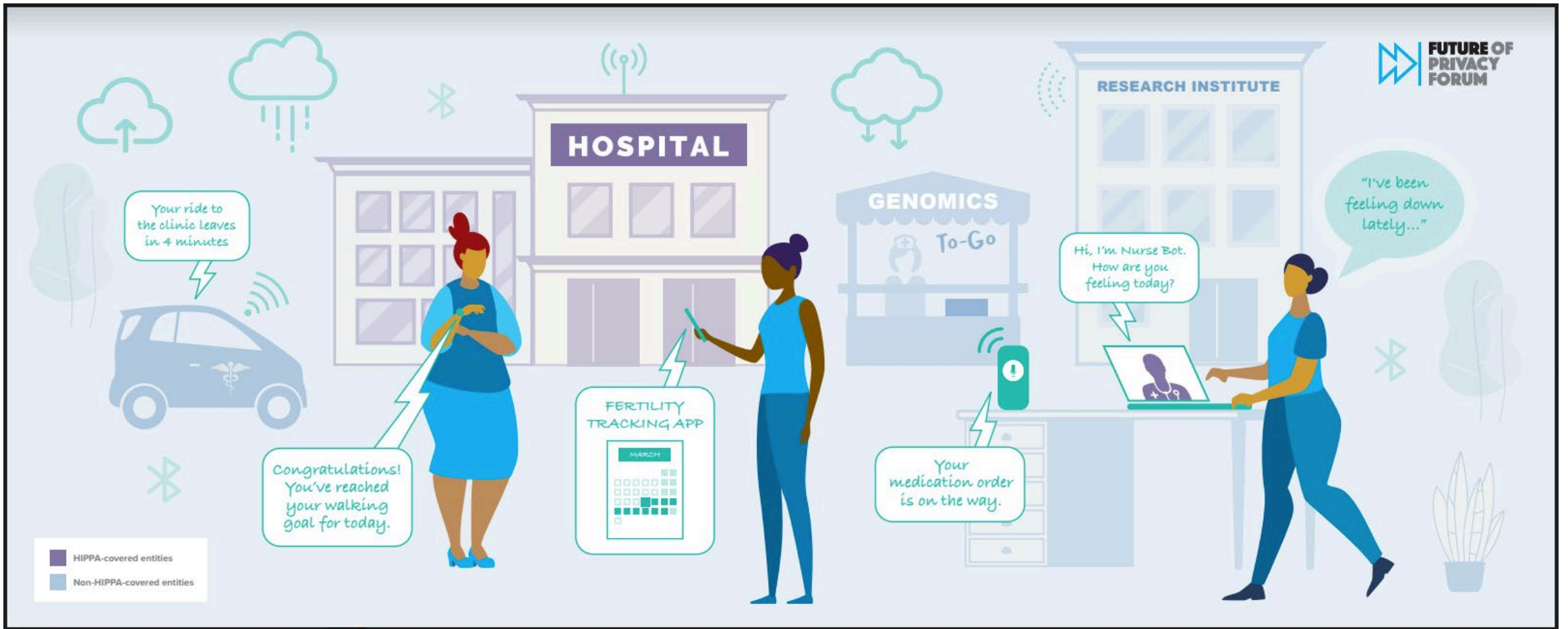**Human-Centered Design**
Center of Excellence

DESIGN PRINCIPLES

Human-Centered Design

- Empathize
- Define
- Ideate
- Prototype
- Test and Iterate

Privacy-by-Design

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default Setting
- Privacy Embedded into Design
- Full Functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Full Lifecycle Protection
- Visibility and Transparency – Keep it Open
- Respect for User Privacy – Keep it User-Centric

Human-Centered Design
Center of Excellence

## Why are Human-Centered Design and Privacy-by-Design Increasingly Important for Health Data?

Sensitive health data is collected across a multitude of remote settings within and outside of the scope of the Health Insurance Portability and Accountability Act (HIPAA). Therefore, health data today warrants privacy protections through governance and privacy-by-design features that consider key human-centered design principles.

PATIENT-CENTERED OUTCOMES

- Patient-reported outcomes (PROs) are patient-centered and convey, in both structured and unstructured formats, patients' symptoms, preferences, complaints, and/or experiences following a clinical intervention.

- PRO measures (PROMs) are quantitative and qualitative data reflecting the health status of a patient, allowing for the data to be used to correlate or predict serious adverse events like hospitalizations for acute and life-threatening symptoms.

- Many entities are exploring ways to:

  - Capture longitudinal PROMs using mobile health technology.

  - Integrate and/or combine PROMs with data from multiple sources like wearable/mobile device data.

Human-Centered Design
Center of Excellence

PATIENT-CENTEREDNESS: FEDERATED LEARNING AS PRIVACY-BY-DESIGN

- Patient reported outcomes measures (PROs/PROMs) data require specific protections when the data is used in or informed by machine learning regimes.

- A patient/human-centered, federated learning architecture for PRO/PROM collection is appropriate to:
  - Ensure the privacy of users' data.
  - Privately track and monitor patients' symptoms, preferences, complaints, and/or experiences following a clinical intervention in real-world settings.
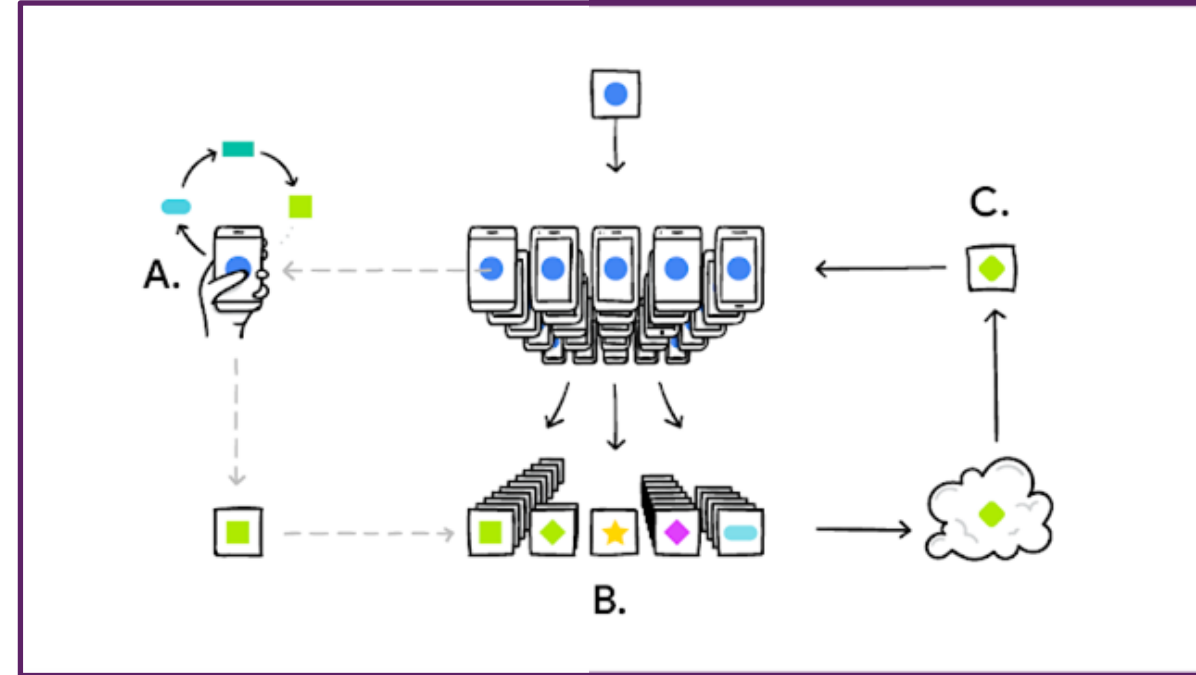
Figure. Google AI illustrates federated learning as "Your phone personalizes the model locally, based on your usage (A). Many users' updates are aggregated (B) to form a consensus change (C) to the shared model, after which the procedure is repeated"
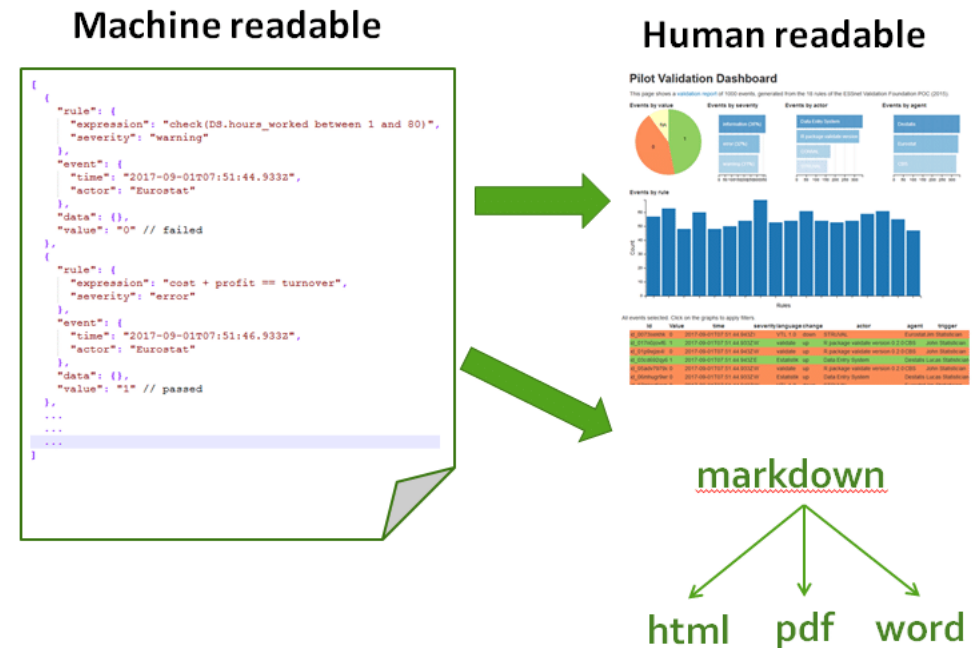
PATIENT-CENTERED OUTCOMES: PRIVACY CONCERNS

- Evidence on the benefits and disadvantages to the electronic capture of PROs shows that **privacy protection, or lack thereof,** is a key disadvantage to the systematic and routine collection of PROMs.

- PROM data shared via mobile apps can reveal fine grained information about a patient or caregiver.

- Therefore, systems using such data should adopt:

  ✓ A nuanced approach to creating and implementing human- and machine-readable **privacy policies** and **consent terms** to uphold patient trust.

Human-Centered Design
Center of Excellence

MACHINE-READABILITY: PRIVACY POLICIES AND CONSENT

In federated learning architectures collecting PROs/PROMs, machine-readability is as important as human-readability to ensure:

✓ Privacy policies ensure that meta-apps are useful and operate well.

✓ Consent terms allows for:
- Consent tools to become data themselves.
- Searchable queries to capture any spectrum of patient preferences when express consent is offered in a nuanced way.

Machine readable

Human readable

Pilot Validation Dashboard

markdown

html pdf word

Human-Centered Design
Center of Excellence

DATA SECURITY REMAINS IMPORTANT

- On-device PROM tools that use machine learning may employ the best privacy policies or consent mechanisms, but may ultimately leave key components, such as the security dimensions, of privacy up to the user.

- Use of a federated learning approach to ensure privacy without attention to security dimensions of private data management may compromise users' data unexpectedly.

- On both client-side and server-side learning, there must be a reasonable expectation that regular transmission patterns will not open the models for attacks, whether upon the model or upon users' data.

Human-Centered Design
Center of Excellence

SUMMARY OF KEY TAKEAWAYS

Users of machine learning to collect and manage PROs/PROMs should ensure the following:

- ✓ Choices about machine learning models do not open users to attack or undue influence and thus do not open users to liability for interpretation of false responses.
- ✓ Machine learning models are not compromised and valuable machine learning spending lost to competitors.
- ✓ Machine learning models are tested and validated to ensure quality of unstructured PROM data versus influencing or skewing PROs concerning safety, symptoms, and other important outcomes.

Dr. Rachele Hendricks-Sturrup
Health Policy Counsel

Dr. Sara Jordan
Policy Counsel, Artificial Intelligence and Ethics

CONTACT US

Dr. Sara Jordan email

sjordan@fpf.org

Dr. Rachele Hendricks-Sturrup email

rhendrickssturrup@fpf.org

THANK YOU!