Agenda

- Welcome – Jen Covich Bordenick & Alexandra Givens (5 min)
- Project Context and Overview – Alice Leiter and Andrew Crawford (15 min)
  - What is the Problem We Set Out to Address?
  - Why is this Work so Timely and Important?
- Substance of the Framework – Andrew Crawford (20 min)
  - Definition of the Dataset
  - Protections that Should Apply
  - Limited Exceptions to Those Protections
- Framework’s Accountability Mechanisms – Alice Leiter (10 min)
- Plans for Phase 2 – Alice Leiter (5 min)
- Questions? (5 min)
Welcome

Jennifer Covich Bordenick, CEO, eHealth Initiative
Alexandra Reeve Givens, CEO, Center for Democracy & Technology
Project Context and Overview
• Funded by the Robert Wood Johnson Foundation
• Set out to examine the gaps in protection for consumer health information and propose solutions
• Meant to support rather than replace the need for new comprehensive federal data privacy legislation
• Convened Steering Committee made up of experts and leaders representing healthcare, technology, academia, consumers and patients, civil rights organizations, and privacy organizations.
• Through regular workgroup meetings, developed a draft that was publicly released in August
• 30-day public comment period drew several dozen comments
<table>
<thead>
<tr>
<th>Name</th>
<th>Company/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joseph Ashkouti</td>
<td>Change Healthcare</td>
</tr>
<tr>
<td>Jacqueline Baratian</td>
<td>Ascension Health</td>
</tr>
<tr>
<td>Julie Barnes</td>
<td>Maverick Health Policy</td>
</tr>
<tr>
<td>Robert Belfort</td>
<td>Manatt</td>
</tr>
<tr>
<td>William Bernstein</td>
<td>Manatt</td>
</tr>
<tr>
<td>Melissa Bianchi</td>
<td>Hogan Lovells</td>
</tr>
<tr>
<td>Susan Bourey</td>
<td>Yale University</td>
</tr>
<tr>
<td>David Brody</td>
<td>Lawyers' Committee for Civil Rights Under Law</td>
</tr>
<tr>
<td>Rebecca Cady</td>
<td>Children's National Hospital</td>
</tr>
<tr>
<td>Shawneequa Callier</td>
<td>George Washington University</td>
</tr>
<tr>
<td>Joanne Charles</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Henry Claypool</td>
<td>American Association of People with Disabilities Consultant</td>
</tr>
<tr>
<td>Andy Coravos</td>
<td>Elektra Labs</td>
</tr>
<tr>
<td>Corey Cutter</td>
<td>American Cancer Society</td>
</tr>
<tr>
<td>Paul Eddy</td>
<td>Wellmark</td>
</tr>
<tr>
<td>Mary Engle</td>
<td>BBB National Programs</td>
</tr>
<tr>
<td>Shari Erickson</td>
<td>American College of Physicians</td>
</tr>
<tr>
<td>Dani Gillespie</td>
<td>National Partnership for Women &amp; Families</td>
</tr>
<tr>
<td>Tina Grande</td>
<td>Healthcare Leadership Council</td>
</tr>
<tr>
<td>Carlos Gutierrez</td>
<td>LGBT Technology Partnership &amp; Institute</td>
</tr>
<tr>
<td>Rachelle Hendricks-Sturrup</td>
<td>Future of Privacy Forum</td>
</tr>
<tr>
<td>Laura Hoffman</td>
<td>American Medical Association</td>
</tr>
<tr>
<td>Alice Jacobs, M.D.</td>
<td>Convergence Group</td>
</tr>
<tr>
<td>Sean Kennedy</td>
<td>Salesforce</td>
</tr>
<tr>
<td>Jeri Koester</td>
<td>Marshfield Clinic Health System</td>
</tr>
<tr>
<td>Erin Mackay</td>
<td>National Partnership for Women &amp; Families</td>
</tr>
<tr>
<td>Amy McDonough</td>
<td>Fitbit</td>
</tr>
<tr>
<td>Meg McElroy</td>
<td>Ascension Health</td>
</tr>
<tr>
<td>Deven McGraw</td>
<td>Citizen</td>
</tr>
<tr>
<td>Dena Mendelsohn</td>
<td>Elektra Labs</td>
</tr>
<tr>
<td>Ben Moscovitch</td>
<td>The Pew Charitable Trusts</td>
</tr>
<tr>
<td>Brenda Pawlak</td>
<td>Manatt</td>
</tr>
<tr>
<td>Jules Polonetsky</td>
<td>Future of Privacy Forum</td>
</tr>
<tr>
<td>Jessica Rich</td>
<td>Institute for Technology Law and Policy at Georgetown University Law Center</td>
</tr>
<tr>
<td>Alejandro Roark</td>
<td>Hispanic Technology &amp; Telecommunications Partnership</td>
</tr>
<tr>
<td>Rajeev Ronanki</td>
<td>Anthem, Inc.</td>
</tr>
<tr>
<td>Alaap Shaw</td>
<td>Epstein Becker Green</td>
</tr>
<tr>
<td>Ashley Thompson</td>
<td>American Hospital Association</td>
</tr>
<tr>
<td>Lee Tien</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>Charlotte Tschider</td>
<td>Loyola University Chicago School of Law</td>
</tr>
<tr>
<td>Nicol Turner-Lee</td>
<td>Brookings Institution</td>
</tr>
<tr>
<td>Ann Waldo</td>
<td>Waido Law Offices</td>
</tr>
<tr>
<td>Marcy Wilder</td>
<td>Hogan Lovells</td>
</tr>
<tr>
<td>Po Yi</td>
<td>Manatt</td>
</tr>
<tr>
<td>Ashwini Zenooz</td>
<td>Salesforce</td>
</tr>
</tbody>
</table>
Why was this Project Necessary?

• HIPAA covers protected health information when held by providers, payers and their business associates (contractors).

• HIPAA does NOT cover data once it leaves the traditional healthcare system.

• HIPAA does NOT protect data held by an individual or uploaded onto most tech platforms (apps, wearable devices, web browsers).

• Result: vast amount of under-protected health information
  o FTC Act not designed to protect this universe of data
  o State laws are patchy and sometimes conflicting
  o Data often subject simply to companies’ terms of service, which tend to be dense, lengthy, and rarely read or understood

• Codes of Conduct and sets of industry best-practices do not go far enough
Why was this Project Necessary?

- New CMS and ONC final regulations will increase amount of health data flowing from health system to individuals.

- Proposed HIPAA rule aims to increase information sharing with broader array of care-givers without individual consent.

- COVID-19 pandemic has illustrated challenges, including consumer trust, associated with widespread collection and use of health data; shone spotlight on disparities with respect to information use.

- Pre-election momentum on Capitol Hill for new federal data privacy legislation; post-election momentum building, particularly in relation to COVID-19.
Data Addressed by the Framework

**Healthcare System** (Providers, Health Plans and Business Associates)
- **Data Addressed**
  - **Protected Health Information (PHI) as Defined by HIPAA**
    - May generally be used without authorization for treatment, payment and health care operations, or other public interest purposes
    - Other uses and disclosures subject to patient authorization
  - **Minimally Regulated Health Data**
    - Data privacy generally subject to terms and conditions of the technology company
    - Regulated by the FTC under unfair and deceptive practices standard

**Technology Companies**
- Information collected by apps and websites (e.g. heart rate data, Fitbit steps, web searches, wellness surveys)

**Data not Addressed**:
- **De-identified health information**: Patient health information from a medical record that has been stripped of all "direct identifiers" for a particular individual
- **Excluded identifiable health information**: Employment records containing health information; educational records containing health information (subject to FERPA); patients' personal health records that are not available to anyone else
Harms That May Come from a Privacy Violation

- Embarrassment
- Creep into other areas of life: employment, education, etc.
- Inaccurate data
- Discriminatory health treatment
- Lack of autonomy
- Lack of trust in technology/health services
Value Proposition of the Framework

• Bridge to future federal legislation, not a be-all, end-all solution
• Raises the bar for consumer privacy
• Benefits companies and organizations that collect and use health data
• Aids regulators and oversight bodies
Framework

Substance Overview

Andrew Crawford, Policy Counsel, CDT
Our objective was to develop the content of a framework for unregulated consumer health information.

Key elements that we focused on were:

1. Scope of the data to be protected;

2. Identifying specific protections that should apply to consumer health information; and

3. Exploring appropriate exceptions to those protections.
Scoping the Data - What is Consumer Health Information?

Sources of Consumer Health Data

- Data Disclosed Outside of HIPAA
- DNA
- Data Created by Wearables, Health Equipment, and Health Apps
- Data Created by Other Services and Products
- Data that is Created by AI and Advanced Computer Learning
- Aggregated Consumer Data
We embraced a broad definition of “consumer health information” based on purpose and use of data.

- No gaps in coverage – wrap-around protection for consumers regardless of format or entity who holds it.

- Reflects modern data practices, which are complex, opaque, and instantaneous.

- Tech neutral and evolves with time.
This section is intended to categorically prohibit secondary uses of health data that consumers do not ask for or expect.

- Limits the amount of consumer health information collected, disclosed, or used to only what is necessary to provide the product or feature the consumer has requested.
- Data collection, sharing, and use limits carry through to third parties.
- Predicated on clear notice and affirmative consent process.

This approach is more stringent than other voluntary frameworks or legal standards, but we believe health data warrants the protection.
The framework includes limited exceptions for:

- Research
- Emergency Use
- Security and Product Functionality
- Employee Information
- Limited Commercial Purposes
Structure of the Framework
Model & Accountability
Mechanisms

Alice Leiter, Vice President & Senior Counsel, eHI
Structure: Self-Regulatory Program

- Consortium of healthcare and health-tech leaders forms a self-regulatory body that operates independently from, but in alignment with, the FTC.
  - Program is housed in and run by a to-be-selected existing independent organization with experience standing up and running self-regulatory bodies.
- Enforcement handled by the consortium but backstopped by the FTC.
- Voluntary self-certification to hold member companies to the Framework’s standards.
- Individual companies accepted as members.
  - Thorough education and onboarding review at enrollment.
- Requires public commitment.
Accountability Mechanisms

- Annual assessments and audits/reviews; active “spot-check” monitoring on a random sample of members throughout each year.
- Independent monitoring by program staff or other authorized evaluators, including publicly announced cases.
- Active complaint-gathering process.
- Dispute resolution mechanism for resolving consumer complaints or complaints by another company based on the program’s standards.
- Requirement to develop a corrective action plan (CAP) and process to lose certification if CAP fails.
- Penalties for persistent or willful non-compliance with the law and/or the program’s standards, such as suspension or dismissal from the program, and/or referral to the FTC and/or state AG.
- Possibility of FTC and/or state AG enforcement of violation of agreed-to industry standards.
Plans for Phase 2 of Work
Phase 2 Context and Goals

• The pandemic has placed even greater focus on health data and how it is collected, disclosed, and used.
• Priorities for a next phase of work would include:
  1. Advocating for and refining our framework, including further engagement of consumers and consumer groups – particularly those representing marginalized communities.
  2. Advancing the framework from a proposal into a more fully developed self-regulatory initiative, including selection of a group to house it and recruitment of individual members; and
  3. Exploring in detail the ways in which the framework’s standards and the program’s design should and can address inequities in the use of consumers’ health-related information.
Questions?
Many Thanks