Release of the *Draft Consumer Privacy Framework for Health Data*

August 26, 2020

Agenda

- Welcome
- Introduction and Project Overview
- Substance Included in the *Draft Framework*
  - Definition of the Dataset
  - Protections that Should Apply
  - Limited Exceptions to Those Protections
- Structure of the *Draft Framework*
  - Proposed Model
  - Accountability Mechanisms
- Next Steps
- How to Provide Feedback on the *Draft Framework*

Welcome

Jennifer Covich Bordenick, CEO, eHealth Initiative

Alexandra Reeve Givens, CEO, Center for Democracy & Technology

Introduction and Project Overview

Project Overview

- Funded by the Robert Wood Johnson Foundation, this project is designed to develop support for a voluntary framework to ensure the privacy of consumers' health data that falls outside the protection of HIPAA
- Goals are to:
    1. Examine the nature of unregulated health data and its implications for consumers and companies;
    2. Propose and review potential approaches for resolving the problem, in the absence of comprehensive federal privacy legislation; and
    3. Identify preferred pathways for industry action
- Steering Committee made up of experts and leaders representing healthcare, technology, academia, consumers and patients, civil rights organizations, and privacy organizations.
- Two workgroups formed: Structure and Substance

Value Proposition

Why action is needed:

- 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

Health Insurance Portability and Accountability Act
HIPAA

- Primary and most far-reaching federal health privacy law
- Underlying statute passed in 1996
- Designed to improve the efficiency and effectiveness of the health care system
- Aimed to modernize the flow of information as more of it became digital
- Among other things, required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge

Who and What Does HIPAA Cover?

1. **Covered Entity –** health care providers (doctors), health care plans (insurers), and health care clearinghouses
2. **Protected Health Information (PHI) –** *"individually identifiable health information"* includes demographic and other information related to current or past health status that is created, held, or transmitted by a covered entity or its business associate

→ "*Individually identifiable" is broadly defined*

3. **Business Associate –** a contractor of a covered entity that performs services and handles PHI on its behalf

Who and What Does HIPAA NOT Cover?

- Data created or held by a person or company that is **not** a covered entity or business associate

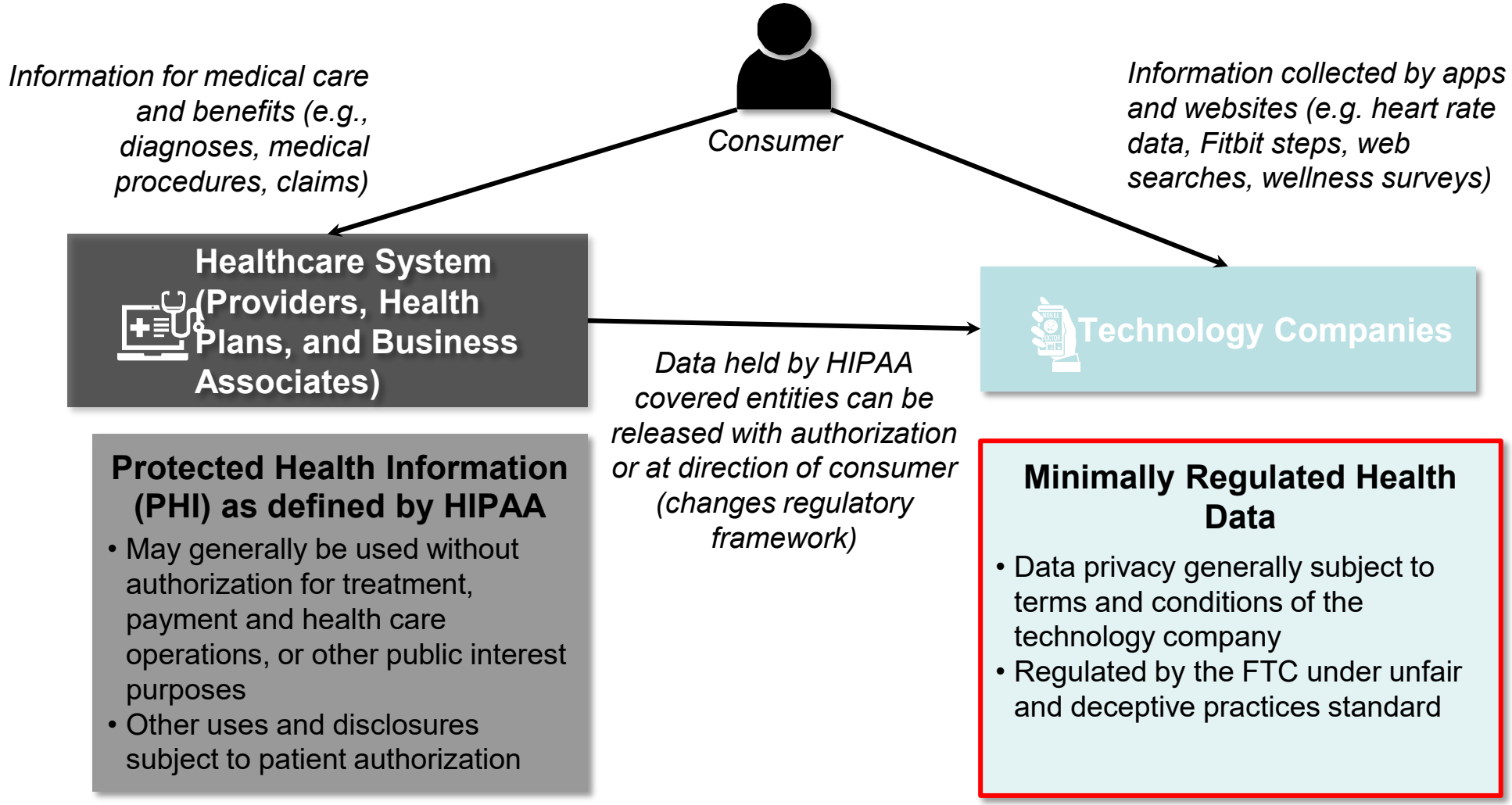
- Data that is **not** individually identifiable

➔ HIPAA defines de-identified data, sets standards on how to de-identify data; places no limits on its use or disclosure

Existing Privacy Laws Do Not Adequately Protect Health Data

- **HIPAA:** Applies to health system only; consumers may wrongly believe that HIPAA applies to other entities or in other contexts
- **Part II Regulations:** Apply to patient information held by federally funded substance abuse treatment programs
- **Common Rule:** Governs federally supported human subjects research
- **FERPA:** Applies to educational records
- **State Laws:** Often contradictory patchwork
- **Federal Trade Commission Act:** Authority to address “unfair” or “deceptive” acts or practices in or affecting commerce
- **GDPR and CCPA:** May not apply given geographic scope; where applicable, can be both under-protective and overprotective

What is the universe of data we are focused on?

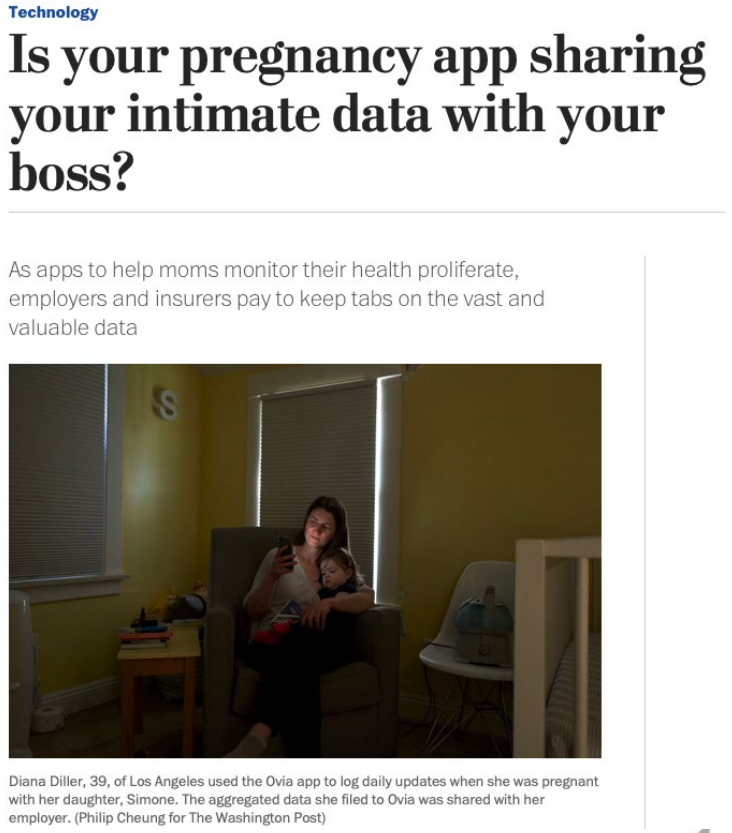


NOT in scope for discussion:

- **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

What are the 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



Technology

Is your pregnancy app sharing your intimate data with your boss?

As apps to help moms monitor their health proliferate, employers and insurers pay to keep tabs on the vast and valuable data

Diana Diller, 39, of Los Angeles used the Ovia app to log daily updates when she was pregnant with her daughter, Simone. The aggregated data she filed to Ovia was shared with her employer. (Philip Cheung for The Washington Post)

Draft Framework

Substance Overview

Andrew Crawford, CDT

Substance Overview

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.

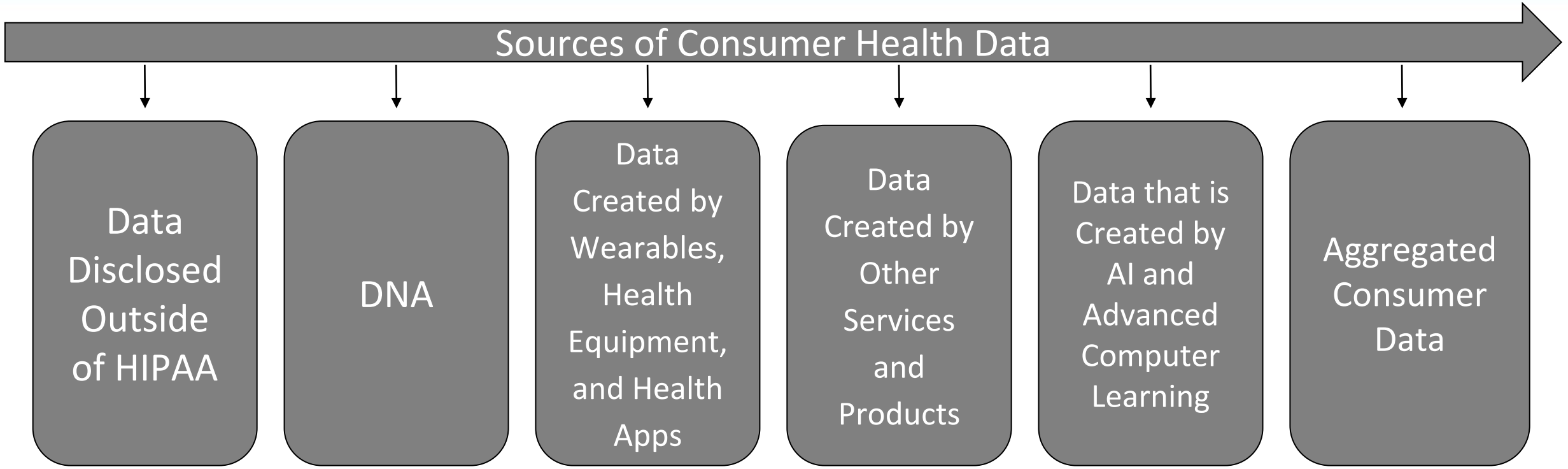
Substance Overview

Our draft goes beyond outdated models that revolve primarily around notice and consent.

- Our draft aims to be consistent with protections found within the GDPR and CCPA.
- Our draft is also designed to complement other frameworks while also filling gaps.

1. CARIN Alliance
2. FTC Best Practices for Mobile Health App Developers
3. Network Advertising Initiative (NAI)

Scoping the Data - What is Consumer Health Information?



Substance Proposal Definition

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.
- Tech neutral and evolves with time.
- Reflects modern data practices: data moves instantaneously, is hard to track, and is fungible.

Substance Proposal
Data Collection and Use

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.

Substance Proposal Exceptions

This draft includes limited exceptions for:

- Research
- Emergency Use
- Security and Product Functionality

Substance Proposal

Deven McGraw
Co-Founder & Chief Regulatory Officer,
Ciitizen

Co-Chair, CDT Advisory Council

Substance Proposal
Thank You

- Many thanks to everyone who devoted time and efforts to helping inform this section.
- This is still a draft.
- We will continue to work on this draft and ensure we have the best approach to protect consumers while also allowing appropriate data use.

Structure of the *Draft Framework* Proposed Model & Accountability Mechanisms

Alice Leiter, eHI

Structure Proposal

- Group began by discussing spectrum of options for action, from do nothing, to developing a new code of conduct or set of best practices, to establishing a self-regulatory program, to proposing new federal legislation

Range of Potential Solutions

DISCUSSION: What types of solutions does the Consumer Privacy Framework Steering Committee seek to address?

Do Nothing / Rely on Existing Regulations and Business Practices

Limited impact: low level of confidence for patients and consumers

Consideration: Would allow additional states to adopt CCPA-like laws, resulting in a conflicting patchwork of laws

Industry-Developed Recommendations on Best Practices & Code(s) of conduct

May result in diffused or competing agendas and consumer confusion

Difficult to ensure accountability and enforcement; limited recourse
Relies on good will and informed companies

Incorporation of provisions into Terms of Service

Industry self-regulatory model with enforcement provisions

Consideration: Creates privacy framework for non-HIPAA health information that protects privacy but forestalls the need for - or serves as a bridge to - additional state or federal legislation. Requires meaningful industry leadership and commitment

Regulatory provisions to clarify and strengthen rules (where possible)

Statutory / New Law

Consideration: comprehensive federal legislation that regulates health information (as an update to HIPAA or new framework) and preempts state laws may take a long time / be difficult to enact in near-term

Structure Proposal

- Coalesced around the idea of a self-regulatory program
- Spent the April meeting, the group's second, discussing various types of self-regulatory programs

Overview of possible self-regulation models in healthcare

	Full Government Enforcement	Quasi-Governmental Organization	Private Sector with Government Support	Private Sector Membership	Private Sector Closed System
	Relies on enforcement of existing laws by FTC and State AGs	Congressional action authorizes an industry body to promulgate and enforce regulations under FTC supervision	Industry consortium, supported by FTC, promulgates and enforces regulations	Subset of industry promulgates and enforces codes and principles for members	Market "gate-keepers" impose rules and requirements for market access
Pros:	*Status quo*	*Legitimacy from FTC oversight; more resources*	*Represents and regulates entire industry; non-participation and non-compliance referred to FTC*	*Monitors/audits members; assists with compliance; can impose fines, refer to FTC and revoke membership*	*Non-compliance is barrier to entry; monitors/audits members; can impose fines*
Cons:	*Limited governmental resources; potential for politicized enforcement*	*Highly improbable due to required actions*	*Voluntary compliance; cannot impose fines*	*Scope limited to members; unable to establish industry-wide norms*	*Least inclusive; broader industry cannot shape rules*
Req Actions:	*None*	*Congressional action; form membership organization representative of entire industry*	*Form coalition of healthcare and health-tech leaders*	*Form membership organization of healthcare apps and technology companies*	*Form coalition of leading app stores*
Examples:	*Status Quo*	*FINRA*	*DAA, NAD*	*NAI*	*PCI/DSS; Apple App Store; Google Play Store*

Structure Proposal

- Agreed that a private membership model with the backstop of government support (FTC) made the most sense
  - Consortium of healthcare and health-tech leaders forms a self-regulatory body that operates independently from, but in alignment with, a federal regulatory agency
  - Enforcement handled by the consortium but backstopped by the FTC
  - Compliance voluntary

Structure Proposal

- **Mary Engle**, Executive Vice President, Policy, BBB National Programs
- Until January 31, 2020, she was the Associate Director of the Division of Advertising Practices at the Federal Trade Commission (FTC)

Highlights of Proposed Model

- Reviewed and discussed a “strawman proposal,” which has since been refined with extensive input from individual workgroup and Steering Committee members
- Key tenets of this proposal include:
  - Self-certification program designed to hold member companies to a set of standards (Substance Workgroup)
  - Accepts individual companies as members, which undergo thorough onboarding review at enrollment and education as to the self-regulatory framework
  - Requires public commitment
  - Annual assessments and audits/reviews; active “spot-check” monitoring on a random sample of members throughout each year
  - Annual fees to maintain this program, with amount on a sliding scale, based on the size of the company in terms of gross sales

Highlights of Proposed Model

- Accountability mechanisms would include:
  - Independent monitoring by program staff or other authorized evaluators, including publicly announced cases;
  - Penalties for persistent or willful non-compliance with the law and 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;
  - Active complaint-gathering process;
  - A 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.

Open Issues for Discussion

- How to define entities for inclusion in the program
- Governance details, including:
  - Whether the program should be run by a brand-new entity or should an existing entity – such as BBB National Programs – run it?
  - How to ensure that certification doesn't disproportionately favor certain types of business over others
  - How to achieve public awareness and trust
- Logistics:
  - Program funding, sustainability, and how would fee structure be designed
  - At what level should certification be – company or product?
- Enforcement – too heavy? Not meaningful enough? What are the penalties?

Next Steps

Next Steps

- Public feedback solicited, reviewed and incorporated
- Ongoing work with and review by Steering Committee
- Drafting of final report
- Final *Framework* released publicly in late fall 2020

How to Provide Feedback

Providing Feedback

- We are looking for feedback on all aspects of the *Draft Framework*, including the areas highlighted in the presentation.
- Comments will be accepted until **Friday, September 25, 2020.**
- To submit comments, please email Alice Leiter at eHI (alice@ehi.org) or Andy Crawford at CDT (acrawford@cdt.org), or visit www.ehidc.org or www.cdt.org.
- eHI and CDT will review all comments received, discuss with the Steering Committee, and incorporate feedback as appropriate.

Many Thanks