National Committee on Vital and Health Statistics
Advising the HHS Secretary on National Health Information Policy

Project Scoping: PCS 2020-2021 Work Plan

NCVHS Subcommittee on Privacy, Confidentiality and Security

March 25, 2020

Today's Agenda

10:45 a.m.:	**Possible Areas of Focus**
11:00 – 11:10 a.m.:	**Scope of Problem**
11:10 – 12:00 pm:	**Themes Discussion**
12:00 – 12:15 pm:	**Next Steps**

Potential PCS Focus for 2020-2021

A) Trusted public health surveillance infrastructure in the face of new pandemic threats.

B) Unexpected or unintended consequences of interoperability rules requiring HIPAA-covered providers to transfer data to non-HIPAA covered entities.

C) Secondary topics:

1) Artificial intelligence
2) Data on opioid and substance use disorder
3) Standards for terms of service of health apps
4) Conflicts between transparency and data protection
5) Research agenda on de-identification methods

Scope of the Trusted Public Health Surveillance Infrastructure (Topic A)

1) Technology: actual and potential affordances
2) Clarifying emergency exceptions to extant rules governing data collection, analysis, and use
3) Secondary uses
4) Ethics and bias
5) Security of data
6) Patchwork of laws

Topic A, Theme 1: Technology's actual and potential affordances

a. International examples

1) Singapore
2) Taiwan
3) China
4) Israel
5) European Data Protection Supervisor

b. Domestic Proposals

1) Telecom data
2) Extant corporate data
3) Special app data

Theme 2: Emergency Exceptions

- These are very helpful to accelerate proper data sharing.
- However, stakeholders may:
  - Desire more clarity in advance with respect to scope of exceptions
  - Need guidance after the emergency with respect to the use or disposal of data collected or shared during the emergency.

Theme 3: Secondary Data Uses

- Several privacy advocates have argued that data gathered via novel monitoring and surveillance infrastructures should:
  - Only be used for public health purposes
  - Be deleted once the emergency is over
- Research advocates may wish to secondarily use the data for research.
- Other secondary uses?
  - Permitted
  - Forbidden

Theme 4: Bias, Ethics

- **Problems**
  - Selective use of data
  - Lack of transparency
    - Complaints about Alipay Health Code from Ant Financial in China
  - Inaccurate data
    - Paul Ohm critique of “Google Flu Trends” (2013)
  - Premature release of improperly anonymized data
    - Current concerns about South Korean “footpath” data
- **Potential solutions**
  - Singapore app based on Bluetooth, not location, data
  - AI ethics literature on representative and fair data sets

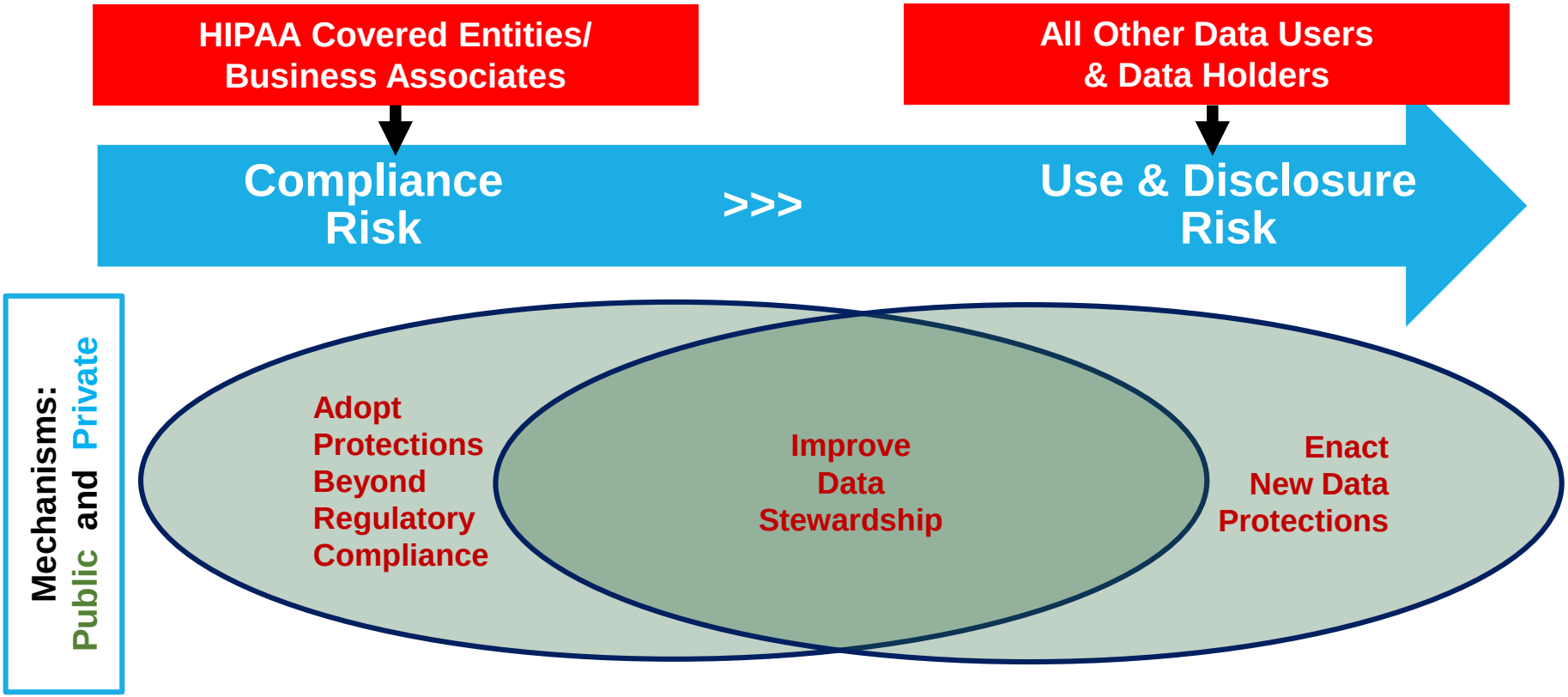
Theme 5: Security

- Sensitive data and database interoperability may require higher standards.

Theme 6: Patchwork approach

The US has a patchwork of laws relating to public health surveillance including HIPAA; public health laws; and state, local and tribal laws; however, in the event of a public health emergency, there is no coordinating mechanism to ensure that they do not conflict.

Scope of “Beyond HIPAA” Work



Health Information Stewardship Continuum

HIPAA Covered Entities and Business Associates | **Data users not covered by HIPAA**

Compliance Risk* >>> Use and Disclosure Risk**

Private

Public

Adopt Protections beyond regulatory compliance

- HIPAA covered entities (CEs) should require data sharing and use agreements before releasing PHI
- CEs could strengthen their risk management practices and de-identification policies of their datasets
- CEs could improve patient transparency regarding uses and disclosures of their data
- Federal expansion of definition of business associates
- FDA requires privacy and security functionality for approved devices

Improvements to Data Stewardship

- With greater understanding, consumers could proactively exercise their rights to privacy and confidentiality of their data
- Data holders should improve their adherence to Fair Information Practices Principles
- Organizations could elect to voluntary certify data holders, applications, and device manufacturers
- Standards Developing Organizations (SDOs) could strengthen standards for data management, privacy and security
- Agencies could issue enhanced sub-regulatory guidance on practices for managing PII and more robust best practices for de-identification.
- FTC enforcement of breach notification rules and app guidance could be strengthened
- Organizations could adopt certification and accreditation of PII data holders

Enactment of New Data Protections

- Consumers should proactively demand greater choice and protection of their information
- FTC could be given greater authority to promulgate more stringent regulation
- Congress could adopt a Federal Data Protection Law
- Congress could expand HIPAA and the definition of covered entities
- States could better regulate data protection

* Compliance risk is exposure to penalties and/or corrective action when an HIPAA-covered organization fails to act in accordance with laws and regulations, internal policies or prescribed best practices.

** Use and disclosure risk is disclosure risk can be defined as the risk that a user or an intruder can use or access a protected dataset to derive confidential information on an individual among those in the original dataset.

Suggestions for NCVHS PCS 2020-2021 Work Plan

Primary focus: Trusted public health surveillance infrastructure in the face of new pandemic threats.

Secondary focus: Unexpected or unintended consequences of interoperability rules requiring HIPAA-covered providers to transfer data to non-HIPAA covered entities.