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

Beyond HIPAA: Stewardship 'By Design' as applied to data, device, and app exemplars

NCVHS Subcommittee on Privacy, Confidentiality and Security

September 2018

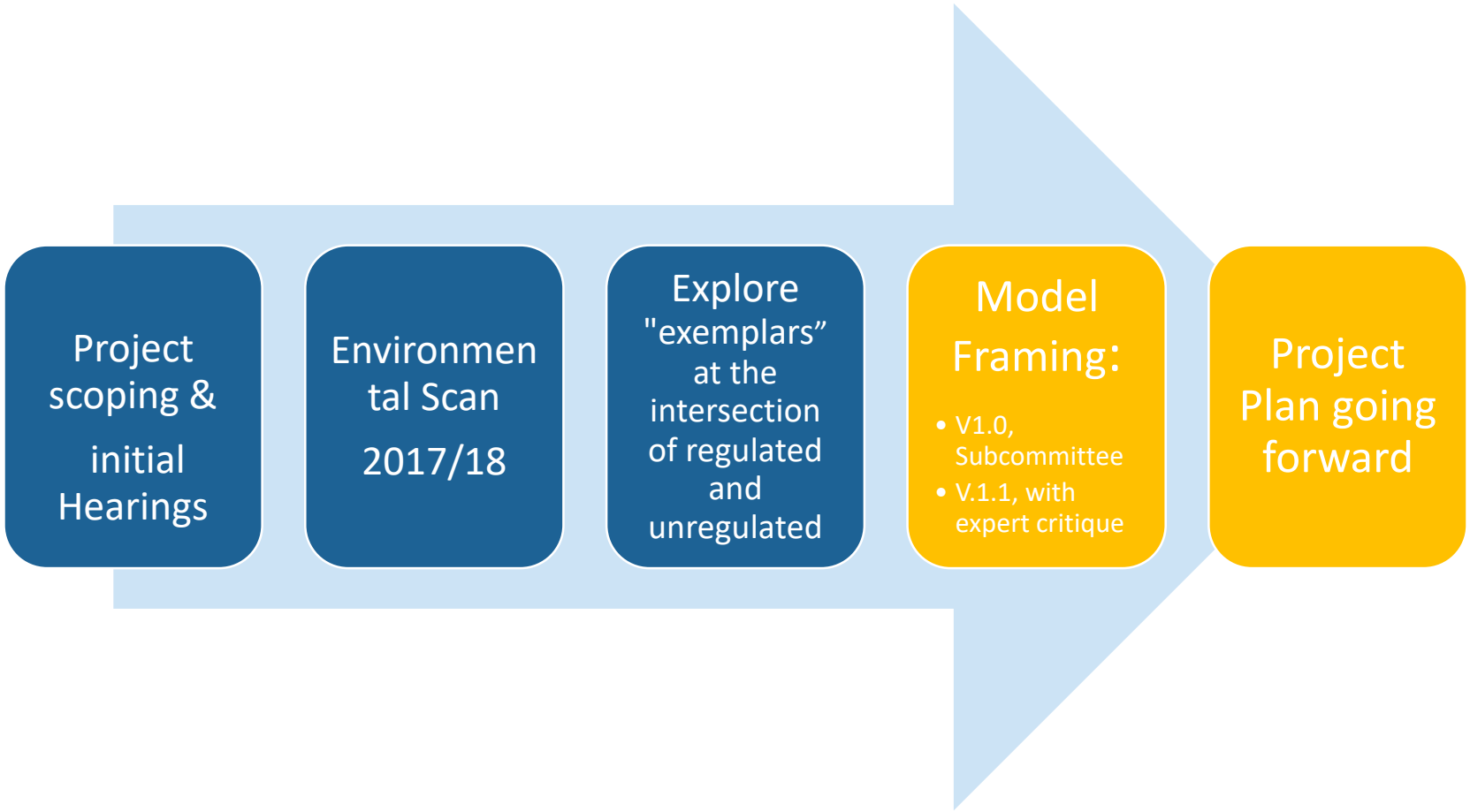
Beyond HIPAA Initiative

Builds on NCVHS's past work and the work of other government and private initiatives to consider a health data privacy and security framework for 21st century health information challenges.

Goals:

- Identify and describe the changing environment and the risks to privacy and security of confidential health information; highlight promising policies, practices and technology;
- Lay out integrative models for how best to protect individuals' privacy and secure health data uses outside of HIPAA protections while enabling useful uses, services and research;
- Formulate recommendations for the Secretary on actions that HHS and other federal Departments might take; and
- Prepare a report for health data stewards.

Progress to Date



Problems Arising from Processing of Personally Identifiable Information (PII)*

NISTIR 8062
An Introduction to Privacy Engineering and Risk Management in Federal Systems
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Risk Assessment

Privacy Risk Factors

Likelihood
a contextual analysis that a data action is likely to create a problem for a representative set of individuals

Impact
An analysis of the costs should the problem occur

NISTIR 8062
An Introduction to Privacy Engineering and Risk Management in Federal Systems
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Beyond HIPAA: Health Information Stewardship Continuum

HIPAA Covered Entities/ Business Associates

Data users not covered by HIPAA

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

Risk

A measure of the extent to which an entity or individual is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impact that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

(NIST SP 800-30 Rev1, supra note 44 at p. 8-13)

* 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.

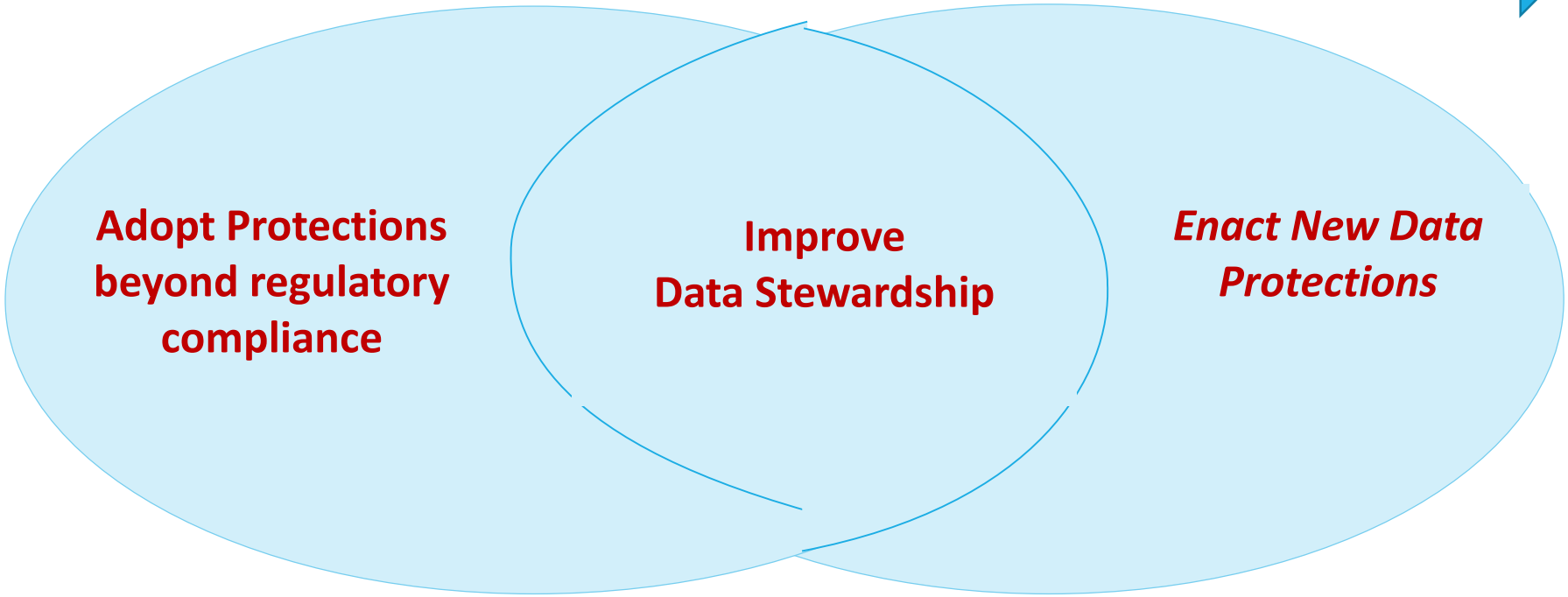
** Use and disclosure risk is the risk that a user or an intruder can use or access a protected dataset to derive confidential information on an individual among those in the original dataset.

Beyond HIPAA: Health Information Stewardship Continuum

HIPAA Covered Entities/
Business Associates

Data users not covered by HIPAA

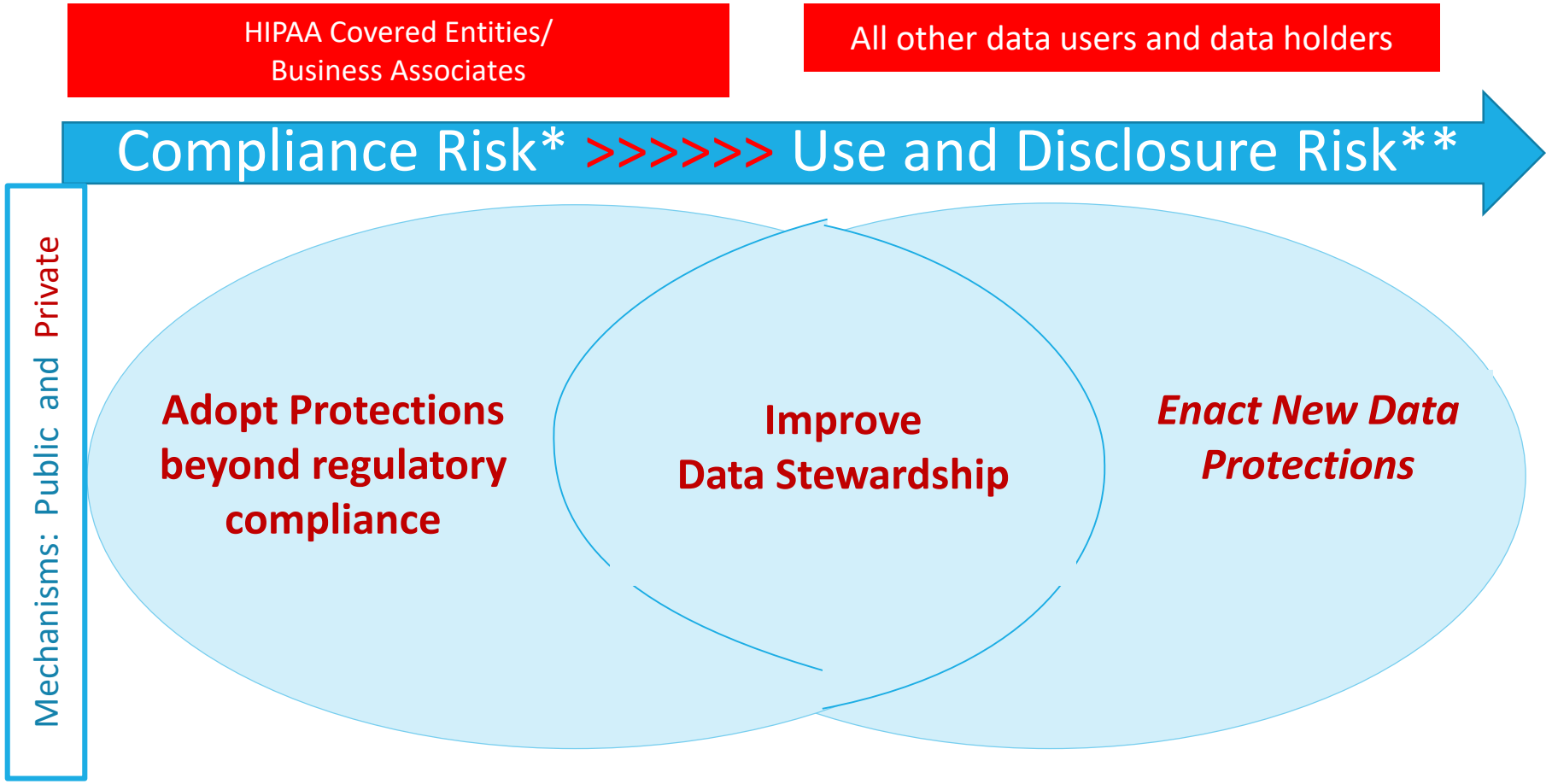
Compliance Risk* >>>>>> Use and Disclosure Risk**



* 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.

Beyond HIPAA: Health Information Stewardship Continuum



* 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.

Beyond HIPAA: 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

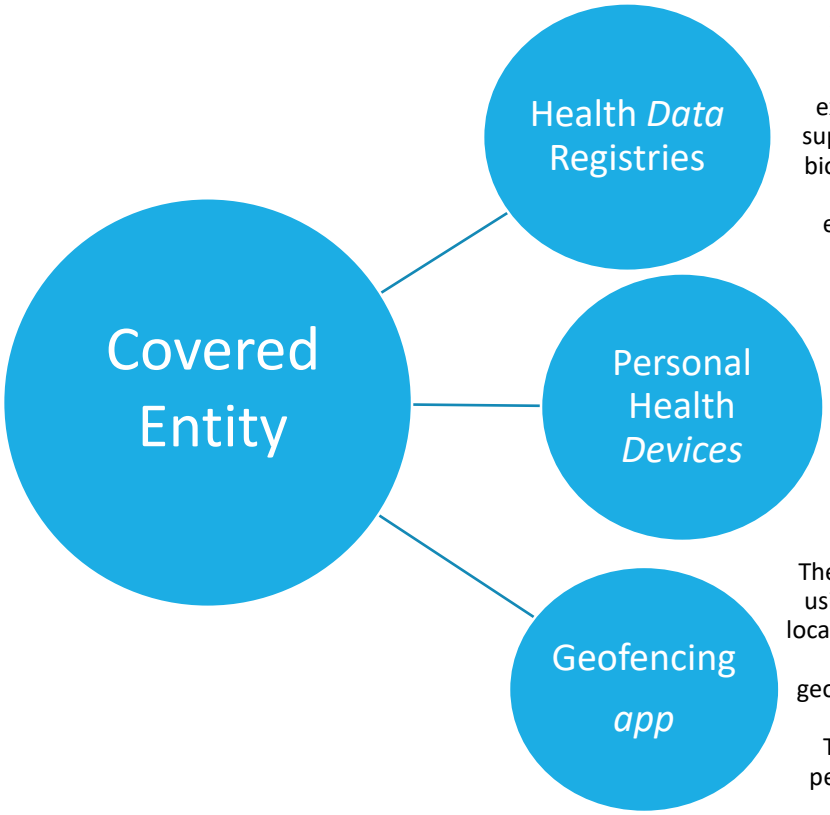
Enactment of New Data Protections

- 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.

Applying the Draft Model to Use Cases Operating at the intersection of the HIPAA-covered and unregulated health data world



A database storing clinical information collected as a byproduct of patient care existing in various forms and support functions ranging from biomedical informatics, clinical research, public health, epidemiology and evidence based clinical practice *

Personal Personal Health Device (PHD) is a term defined by IEEE to mean a health device which is normally used for measurement by a chronic patient, especially seniors, for telemedicine at home and in other buildings.**

The technology identifies people using cellphones within a certain location and then targets them with ads. In the health space, geofencing is used to market legal services to ED patients and Targeting other messaging to people who visit clinics or other health facilities ***

- Drolet, BC and Johnson, KB. Categorizing the world of registries. Journal of Biomedical Informatics 41 (2008) 1009-1020: https://www.sciencedirect.com/science/article/pii/S1532046408000018X?via%3Dihub

** ISO/IEEE, 11073-20601: health informatics—personal health device communication, application profile optimized exchange protocol, http://www.iso.org.

***https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers

CRITIQUE MECHANISMS

Use Case: Registries

	Leverage Current Mechanisms	Improve data stewardship	Enact new protections
Private	• Covered entities requires data use agreements which include prohibitions against reidentification and redisclosure. • Covered entities offer patients opportunity to opt out of registries. • CEs strengthen management of de-identified data sets	• Voluntary certification of registry sponsors	
Public	• OCR issues guidance for registry BA and DUAs	• Mechanism for accreditation of registries for funding streams	• Registries become covered entities

CRITIQUE MECHANISMS

Use Case: Personal Health Devices

	Leverage Current Mechanisms	Improve data stewardship	Enact new protections
Private	• Covered entities and device manufacturers voluntarily enter into BA agreements before use of patient generated data • Ces expand patient education about registry uses	• People given more information about device data sharing • Voluntary certification of device manufacturers	
Public	• OCR issues guidance for BAs with device manufacturers • FDA requires privacy and security functionality for approved devices	• Mandatory certification of device manufacturer	FTC adopts regulations for device manufacturers

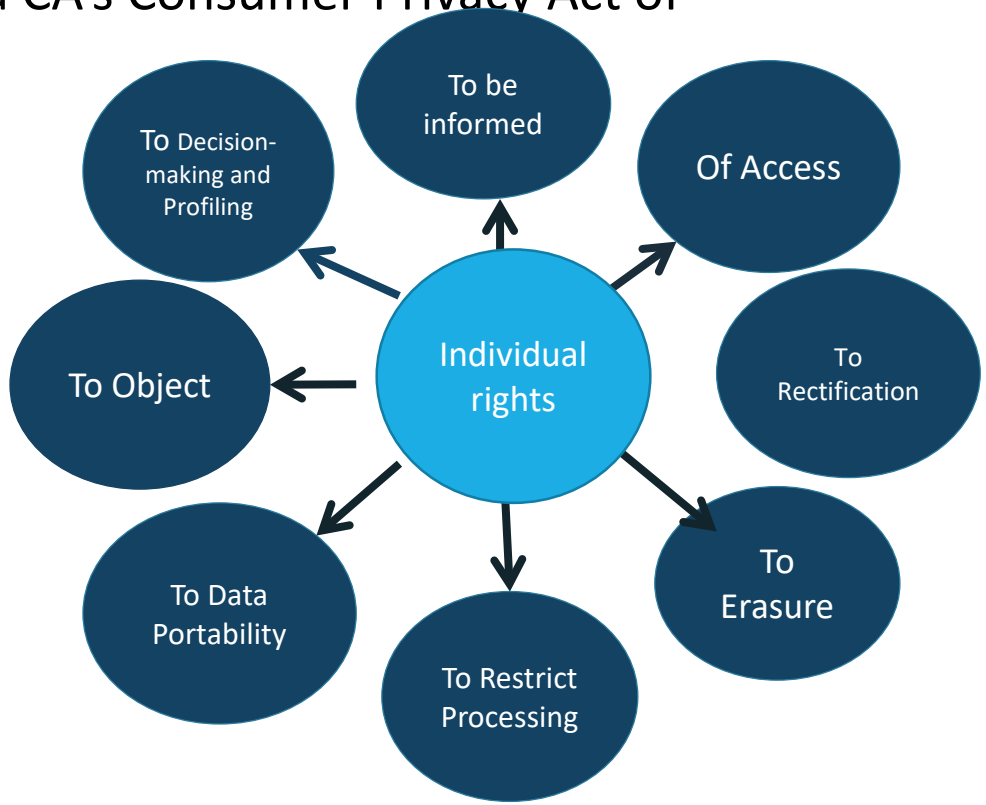
CRITIQUE MECHANISMS

Use Case: Geofencing apps

	Leverage Current Mechanisms	Improve data stewardship	Enact new protections
Private	• Covered entities step up information to patients about risk of using location features in EDs		• People proactively demand greater choice and protection of their information
Public		• Broader enforcement of breach and use of data from apps	• Congress adopts Federal Data Protection Laws • State regulate data protection

Principles on which this Model Rests

- Professional Codes
- Derived from Fair Information Practice Principles (various NCVHS products)
- Right of Data Subjects per GDPR and CA's Consumer Privacy Act of 2018



Themes for 13th Report to Congress

- The Regulated and Unregulated Worlds
  - Strengths of HIPAA's privacy and security approach and its growing limitations;
  - Need for strategic changes to protect individuals from risk of harm "beyond HIPAA"
- Selected stories of the world beyond HIPAA illustrating potential risks and harms pertaining to (draw from Beyond HIPAA Report and the Report of the Cybersecurity Task Force:
  - Big data
  - Personal health devices and the Internet of Things
  - Security
- Consumer attitudes –reinforce points made in 12th Report
- Opportunity to increase protections and choice for consumers and at the same time reduce burden
- Framing legislative issues