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

Health Information Privacy Beyond HIPAA: A Framework for Use and Protection

Bill Stead, NCVHS Chair
Linda Kloss, Former Chair, Privacy, Confidentiality and Security Subcommittee

October 17, 2019

Today's Presentation

- Review of NCVHS mandate
- NCVHS's Focus on privacy **"Beyond HIPAA"**
- A Proposed **Framework for Use and Protection of Health Information Beyond HIPAA**
- Challenges and recommendations in advancing the Framework

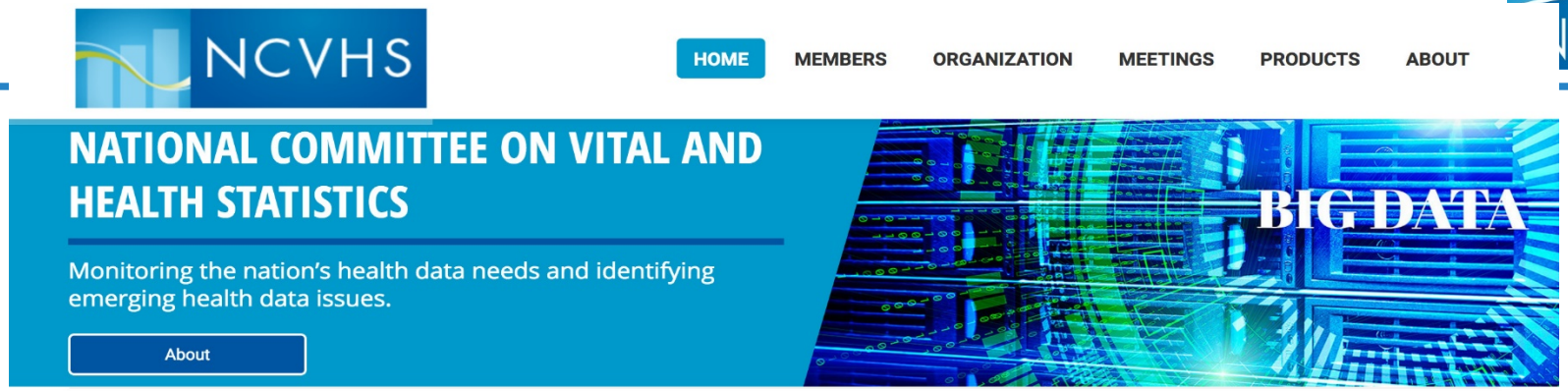
About NCVHS

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory public advisory body to the Secretary of HHS in the areas of health data, standards, statistics, national health information policy, and HIPAA (42 U.S.C. § 242k(k)).

From the Charter:

"Study and identify privacy, security, and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data."

https://ncvhs.hhs.gov/

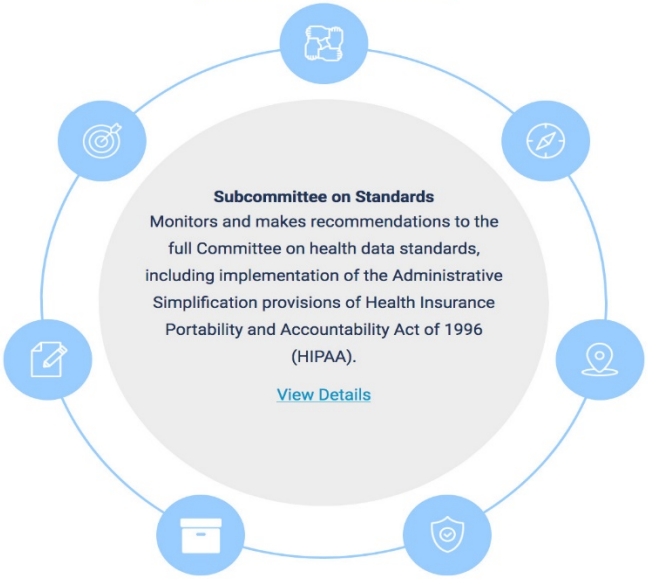


About NCVHS

The NCVHS serves as the statutory [42 U.S.C. 242k(k)] public advisory body to the Secretary of Health and Human Services (HHS) for health data, statistics, privacy, and national health information policy and the Health Insurance Portability and Accountability Act (HIPAA). The Committee advises the HHS Secretary, reports regularly to Congress on HIPAA implementation, and serves as a forum for interaction between HHS and interested private sector groups on a range of health data issues.

MORE ABOUT NCVHS

Subcommittees

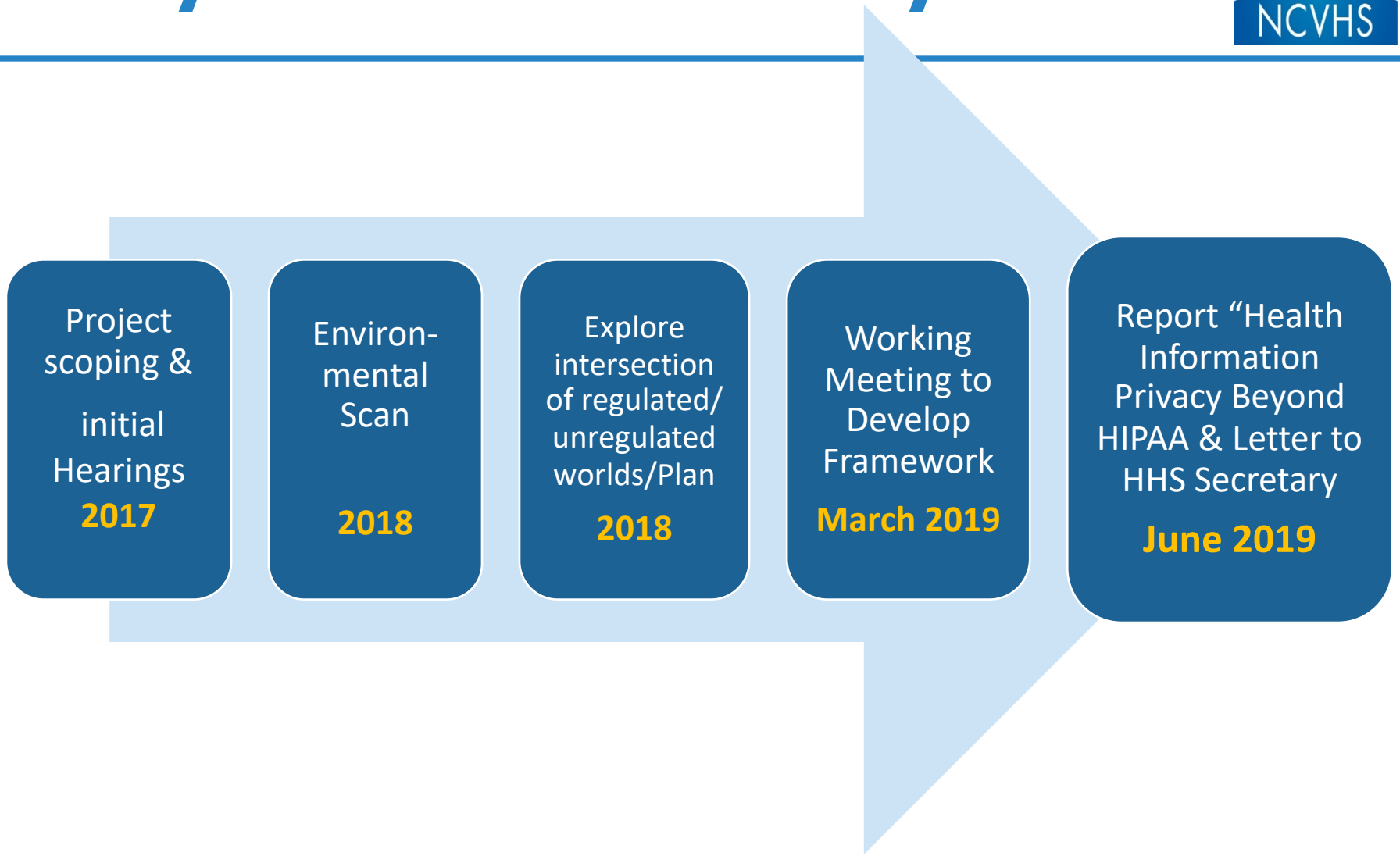


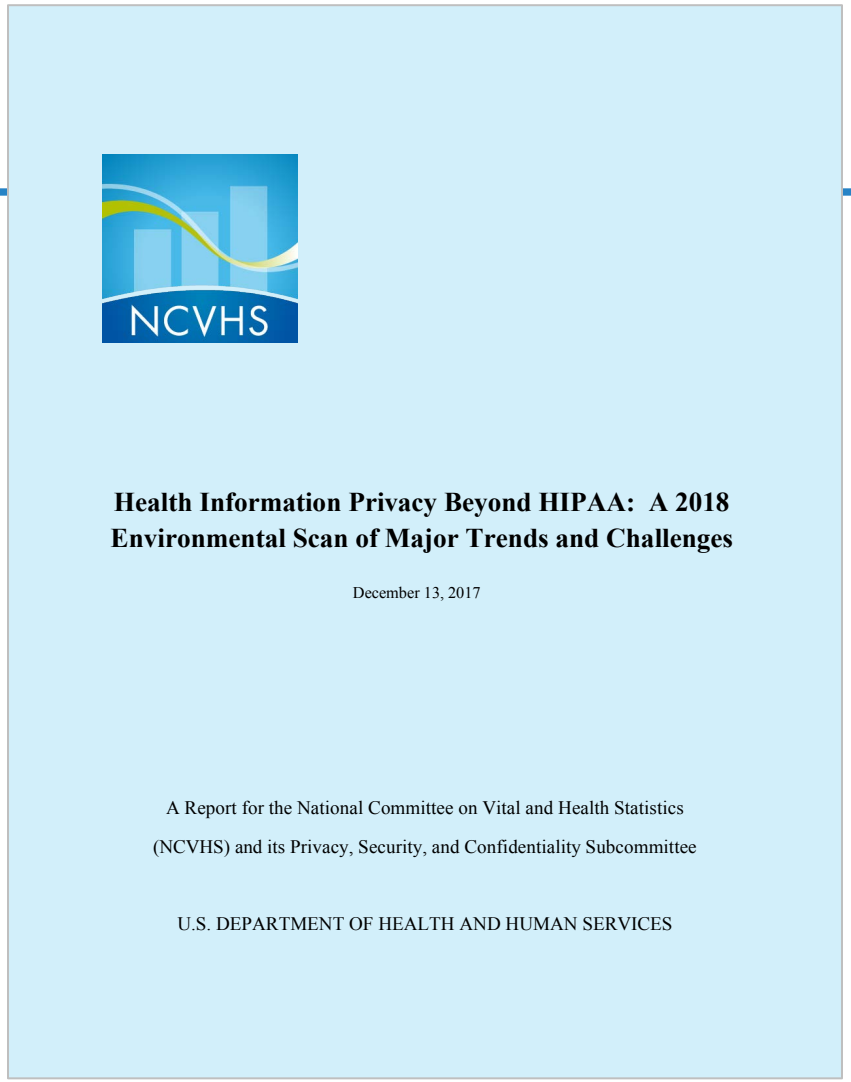
NCVHS' Beyond HIPAA Initiative

Goals:

- Describe the changing risks to privacy and security of confidential health information;
- Lay out integrative models for how best to protect individuals' privacy and secure health data uses outside of HIPAA protections;
- Formulate recommendations for the Secretary; and
- Prepare a report for health data stewards.

Beyond HIPAA Journey





Health information lives in two worlds---*regulated* and largely *unregulated*.

https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

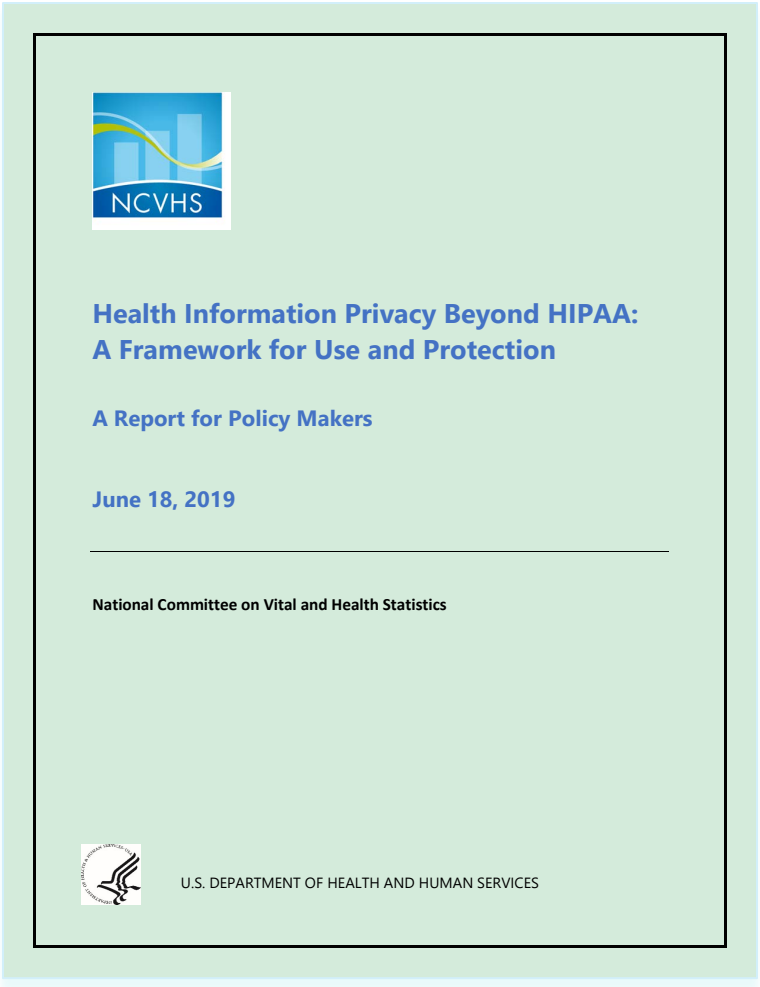
Essential HPIAA Guardrails

1. Health information definition
2. Responsibilities and obligations
3. Rights of information subjects
4. Enforcement

The World Beyond HIPAA – Dilemmas

1. What is health information?
2. Who owns the information
3. What are the rights of information subjects?
4. What are the mechanisms for protecting privacy? To what degree is de-identification a safeguard?
5. What are the rights and responsibilities of data holders or processors?

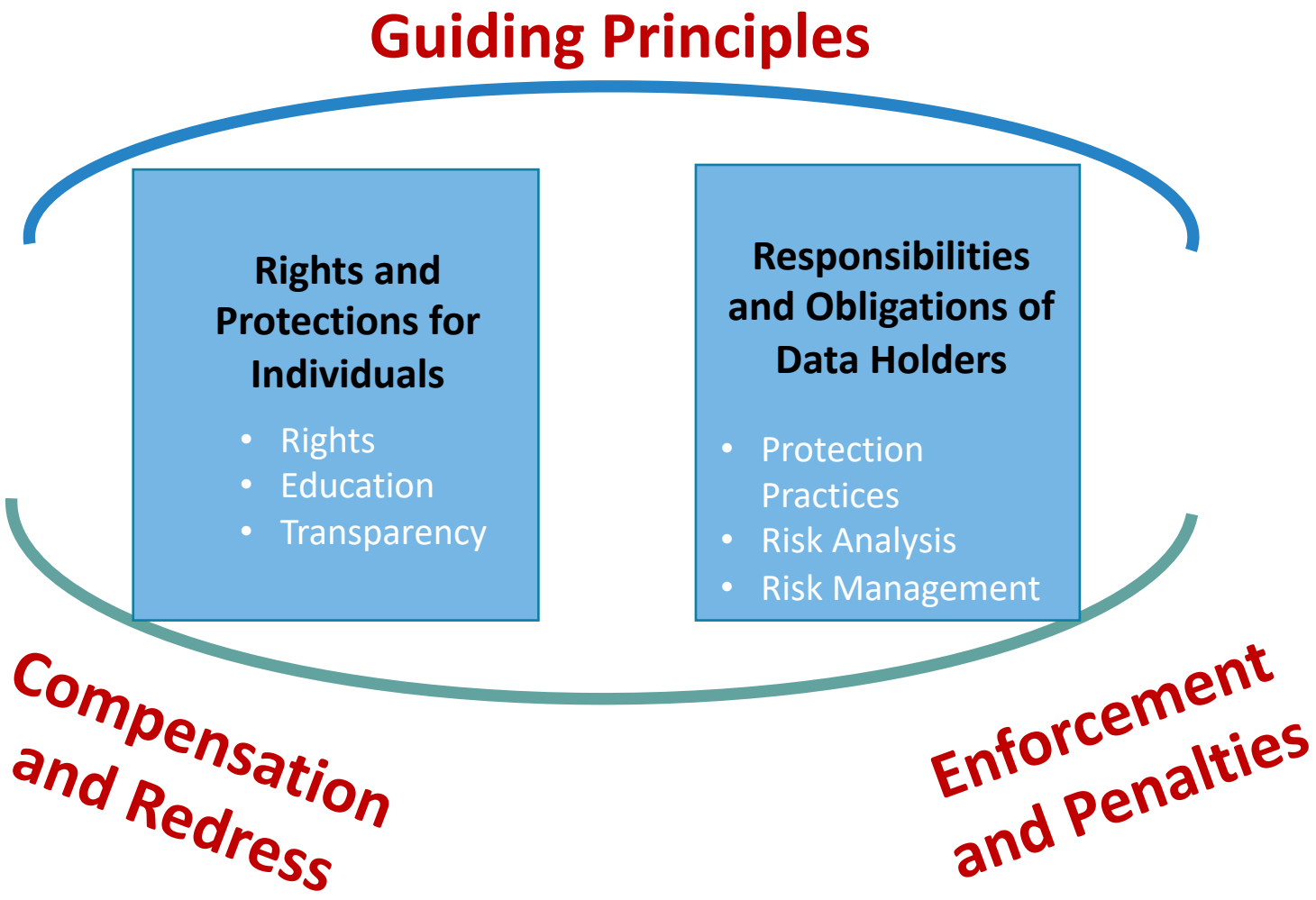
Health Information Privacy Beyond HIPAA: A Framework for Use and Protection



- Guiding Principles for Use and Protection
- Framework for Use and Protection
- The Path Forward

https://ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdf

Framework for Use and Protection of Health Information Beyond HIPAA



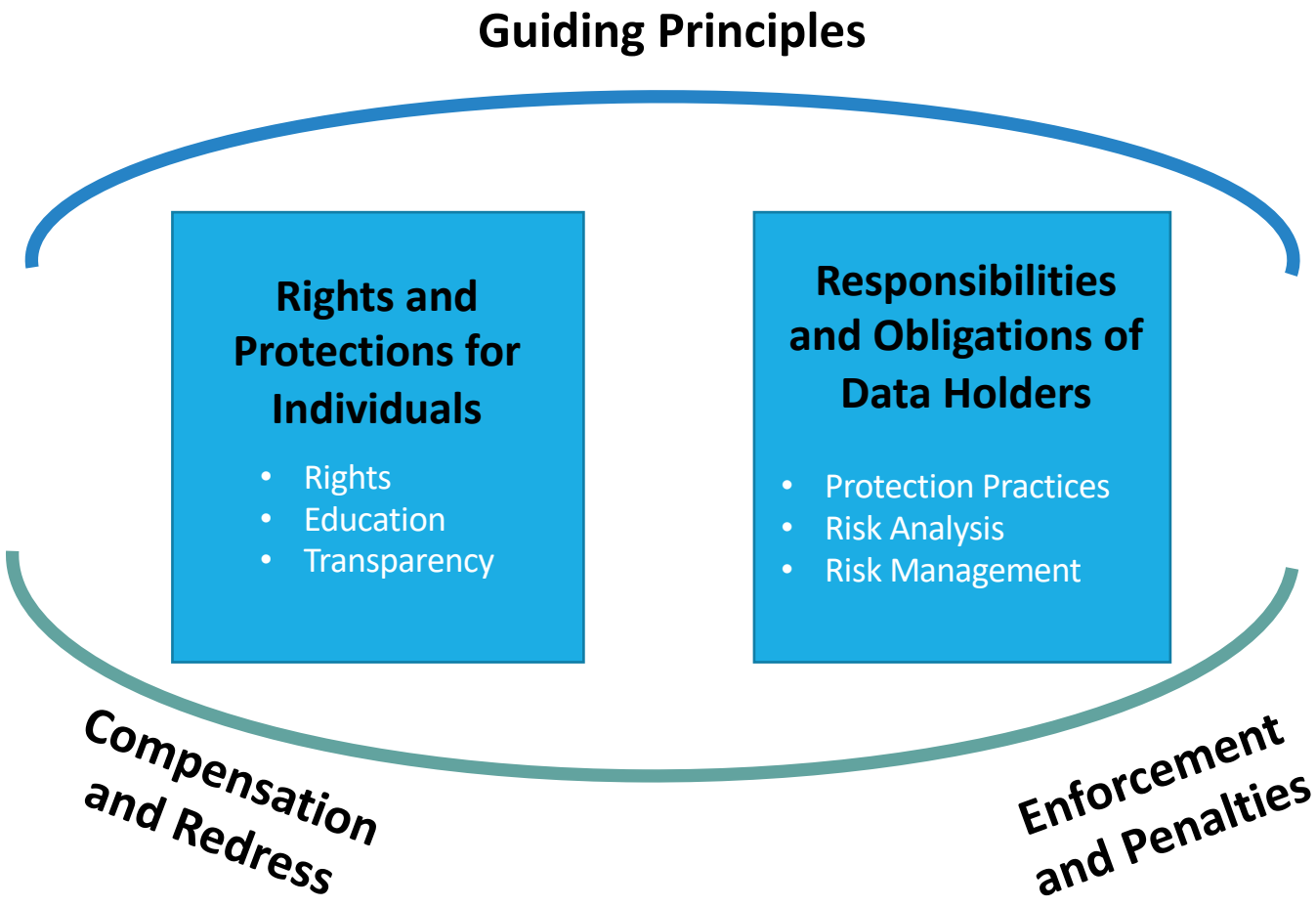
Guiding Principles for Use and Protection of Health Information

1. Privacy protections should promote greater health equity.
2. Individuals should have options to exercise their privacy preferences and assert information rights.
3. Data holders should disclose what information they hold, and how it is secured.
4. Data holders should specify the purposes for which information is collected, used, and disclosed.
5. Information collection should be limited to that needed for the current purpose.

Guiding Principles for Use and Protection of Health Information

6. Consent requirements for disclosure should be meaningful and understandable.
7. Unconsented uses and disclosures are limited and clearly specified.
8. Based upon a risk analysis, appropriately rigorous protections are in place for more granular and sensitive information.
9. Data sharing should only occur under a data use agreement which prohibits re-identification and re-disclosure.

Framework for Use and Protection of Health Information Beyond HIPAA



Near Term Actions:
Covered Entities and Business Associates

1. Require data sharing and data use agreements before disclosing individually identifiable health information.
2. Improve informed consent practices.
3. Strengthen de-identification methods and match methods to the sensitivity of the dataset.
4. Improve ease of access for individuals to their information.
5. Become more transparent about the actual uses being made of personally identifiable and de-identified health information.
6. Improve accounting of disclosures including disclosure of de-identified data sets.
7. Implement more robust information and data governance programs particularly focused on access and disclosure management and security.
8. Adopt personal health technology products only if they meet rigorous privacy and security specifications.
9. Educate patients about their information rights and how to access and protect their health information.

Near Term Actions:
Data Holders

1. App developers adopt privacy by design practices and adhere to security best practices.
2. Require data sharing agreements before redisclosing identifiable health information.
3. Implement information and data governance programs to upgrade the policies and practices for managing health information.
4. Improve understanding and adherence to Fair Information Practices Principles.
5. Become more transparent about the actual uses being made of personally identifiable and de-identified health information.
6. Educate employees on health information confidentiality and hold them responsible for breaches or any misuse of information.

Near Term Actions:
Information Subjects

1. Learn about your health information rights and how to exercise them.
2. Be diligent about protecting health information in your possession.
3. Question entities that want your health related information about intended use, resale and redisclosure policies and privacy and security practices.
4. Read and understand consent forms, including electronic consents, before signing them.
5. Consider the rights of family members whose interests may be impacted by your own decisions about your confidential health information.

Near Term Actions:
HHS

1. Establish federal health information privacy and security standards for health data registries that are not covered entities, business associates or operate under other federal or state privacy and security regulations.
2. Establish health information security and privacy standards for medical device and mobile application manufacturers.
3. Develop consumer guidance concerning use and protection of their genetic information when it is not protected by HIPAA.
4. Support a research agenda on de-identification methods including the risks of reidentification related to various methods for de-identification.

Near Term Actions:
HHS and other Federal Agencies

1. Support a federal study of how consumers might exercise their rights of action to seek redress in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was used.
2. Develop a model for tiers or categories of harms and risks regarding unauthorized access or misuse of health information beyond HIPAA.
3. Develop federal baseline standards for privacy and security protection of individually identifiable and de-identified health information held by commercial organizations outside the scope of HIPAA.
4. Develop scalable consumer and school-based education curricula about health information privacy and security.

Many contributors to thank…

- OCR
- NIST
- Experts who provided testimony
- Invited experts who participated in Framework development
- NCVHS and Subcommittee members
- NCVHS staff

Questions & Discussion