



# **Beyond HIPAA Working Meeting**

## **Meeting Summary**

**Held March 21-22, 2019**

---

**Subcommittee on Privacy, Confidentiality and Security**

**National Committee on Vital and Health Statistics**



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

This report was written by staff to the NCVHS Subcommittee on Privacy, Confidentiality and Security (PCS) in collaboration with NCVHS members.

### **NCVHS Members and Staff in Attendance**

Linda L. Kloss, MA, RHIA,\* **Subcommittee Chair**

Nicholas L. Coussoule,\* (by phone)

Vickie M. Mays, PhD, MSPH \*

Jacki Monson, JD \* (by phone)

William W. Stead, MD, **NCVHS Chair**

Alexandra Goss

Debra Strickland, MS

Richard W. Landen, MPH, MBA

\*Member of the Subcommittee on Privacy, Confidentiality and Security

Rachel Seeger, MA, MPA, **Lead Staff, Subcommittee on Privacy, Confidentiality & Security**

Senior Advisor, Public Affairs and Outreach

HHS Office for Civil Rights

U.S. Department of Health and Human Services

Maya Bernstein, JD

Privacy Advocate, Science and Data Policy

Office of the Assistant Secretary for Planning and Evaluation

U.S. Department of Health and Human Services

Rebecca Hines, MHS, **NCVHS Executive Secretary/Designated Federal Officer**

Health Scientist

National Center for Health Statistics, Centers for Disease Control & Prevention (CDC)

U.S. Department of Health and Human Services

Debbie Jackson, MA, NCHS, HHS

Senior Program Analyst

Geneva Cashaw, NCHS, HHS

Committee Management Assistant

**See Appendix A for a complete list of meeting attendees and invited guests.**

## **The National Committee on Vital and Health Statistics**

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory [42 U.S.C. 242(k)] public advisory body to the Secretary of the Department of Health and Human Services (HHS) in the areas of health data, standards, statistics, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C.242k[k]). In this capacity, the Committee provides advice and assistance to HHS and serves as a forum for interaction with relevant private sector groups on a range of health data issues. The Committee is composed of eighteen individuals from the private sector who are distinguished in the fields of health statistics, electronic interchange of health care information, privacy, confidentiality, and security of electronic information, population-based public health, purchasing or financing of health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Sixteen of the members are appointed by the Secretary of HHS for terms of four years each, with about four new members being appointed each year. Two additional members are selected by Congress. [ncvhs.hhs.gov](http://ncvhs.hhs.gov)

May 2019

## Introduction and Background for the Meeting

NCVHS is charged with studying and identifying “privacy and security and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data.” As part of that charge, the Committee advises the Secretary of HHS and reports to Congress on the status of the HIPAA Rules, which establishes the regulatory framework for personally identifiable health information held by covered entities and business associates.

In 2017, the Committee through its Subcommittee on Privacy, Confidentiality and Security (PCS), undertook a “Beyond HIPAA” initiative to examine emerging health information privacy and security issues that are outside of the regulatory scope of HIPAA to consider a health data privacy and security framework for the 21st century. The goals for the Beyond HIPAA initiative are to:

1. Describe the changing environment and identify the risks to privacy and security of confidential health information, highlighting promising policies, practices and technology;
2. Propose integrative models for how best to protect individuals’ privacy and secure health data uses outside of HIPAA protections while enabling important uses, services and research;
3. Formulate recommendations for the Secretary on actions that HHS might take; and
4. Prepare a report for data stewardship.

After hearings on this topic held in 2017 and 2018, NCVHS conducted an environmental scan titled, “Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges,” available on the NCVHS website.<sup>1</sup> The scan described the two spheres of health information: one that is regulated by HIPAA and the other that is largely unregulated. The scan addressed existing and emerging policy frameworks, practices, and technologies in the areas of: big data and analytics, personal health devices, the Internet of Things, and evolving technologies for privacy and security. It also examined privacy and data protection laws in other domains and changing consumer attitudes regarding health information privacy.

The Committee has considered the range of public and private action options to improve health data privacy and security beyond HIPAA focusing first on examples of uses that are at the intersection of the HIPAA regulated and unregulated spheres. These include health registries (populated with health information but often not covered by a business associate agreement), personal health devices, and applications that may exchange information with covered entities or business associates (but essentially operate in the unregulated world). At

---

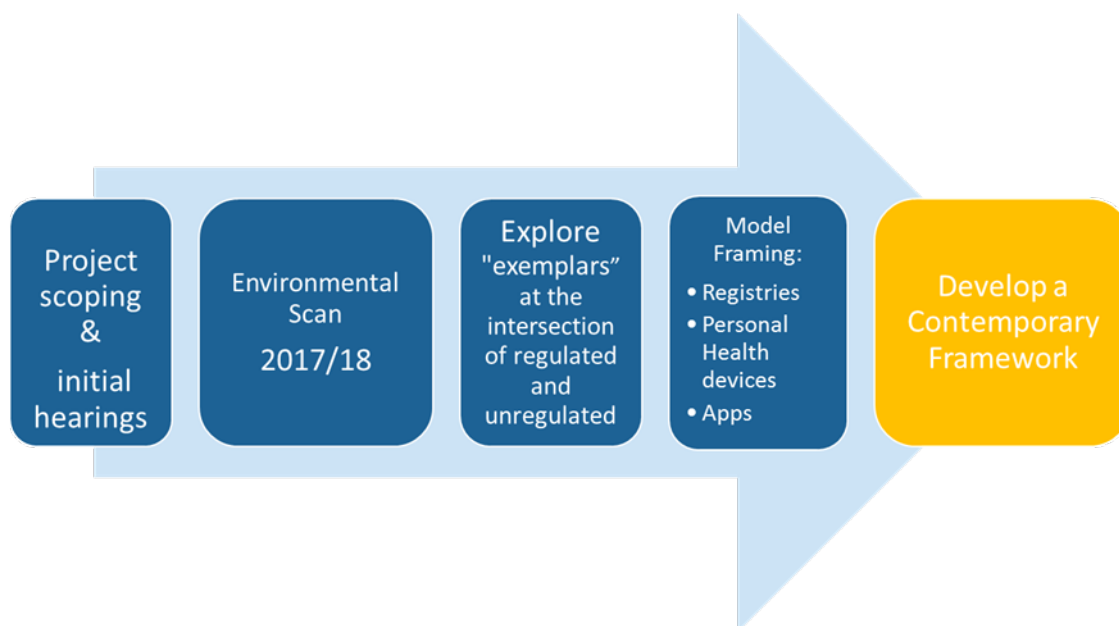
<sup>1</sup> December 13, 2017 Report: Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges, [https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA\\_Report-Final-02-08-18.pdf](https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf)

this juncture, the Committee is moving forward from study of the current environment to formulation of recommendations for action.

## Introductions and Opening Background

To open the March 2019 Beyond HIPAA Working Meeting, NCVHS's PCS Subcommittee Chair Linda Kloss described the meeting objectives within the context of the overall charge of the Committee to advise the HHS Secretary on HIPAA and national health information policy. In her opening remarks, she explained that there is a sea change in how individuals and organizations are using health data outside of the scope of HIPAA and that the time is right to think about the future of meaningful protection of privacy and security architecture in this space. Ms. Kloss then invited participants to introduce themselves and describe the role they play within their respective organizations.

Ms. Kloss defined the goals of the working meeting to build 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. She reviewed the Subcommittee's work over the past two years including project scoping, hearings, and exploring the space Beyond HIPAA that is largely unregulated as health data moves out of the HIPAA jurisdiction, as well as the current landscape of protections required of covered entities and business associate under HIPAA or through other regulations. The Subcommittee looked at several use case exemplars: registries, health apps, and personal health technologies, where there is exchange of information between the regulated and unregulated world. This work produced the draft model that has been used for discussion framing the work at this meeting.



## Meeting Design

Ms. Kloss described the format of the meeting. To supplement the expertise of the Subcommittee, invitations were extended to key guests with particular subject matter expertise in this space. Over the two days, meeting input was used to:

1. Outline key stewardship principles for currently “unregulated” health information and the essential public and private levers to ensure appropriate governance.
2. Build on NCVHS’s past work, reach consensus on themes, important public and private actions, and a pathway forward to be presented in a 2019 policy report.
3. Identify recommendations for actions by the HHS Secretary.
4. Identify key themes for communications with individuals, policymakers, and stakeholders in the private sector.

To provide background and frame the discussion, NCVHS circulated the Environmental Scan report and other supporting materials to members and invited experts more than a month prior to the meeting.

Following the meeting, a report will be developed summarizing key principles and a framework for protecting health information that is not subject to HIPAA and a letter to the Secretary with recommendations for actions.

## Identifying Major Themes

The first meeting exercise on March 21, 2019 was a discussion of major themes in health information privacy where information is digital and outside of the scope of HIPAA regulations. Key questions included: Why are we concerned about this, how do we craft an overarching statement of why this topic is important and why is this the right time to address it? Much has changed in the health information landscape, and there is a new urgency today that did not exist a decade ago with the advent of new technologies such as mobile devices, applications, and the expanding use of big data. Ms. Kloss directed members and guests to spend 15 minutes discussing these questions before moving into specific themes.

Subcommittee members and invited guests offered a range of observations that underscore the breadth of the issues. The following are illustrative examples. The full discussion is available in the meeting transcript<sup>2</sup>:

- There is a new ease of moving data that was originally collected for health care and move it somewhere where it has no HIPAA protections at all.
- There is greater risk today, with less benefit to the individual. The benefit is going to

---

<sup>2</sup> Transcript, March 21, 2019 Meeting NCVHS Privacy, Confidentiality & Security Subcommittee:  
<https://ncvhs.hhs.gov/transcripts-minutes/transcripts-privacy-confidentiality-security-march-21-2019/>

the privacy corporation that is monetizing the data by aggregating it and repackaging it.

- Individuals are freeing their data and sharing it without a full understanding of what this sharing will mean to the person moving forward in the downstream activity.
- Data may have its origins within the HIPAA protections and then move beyond HIPAA protections. There is currently momentum under ONC and CMS's NPRM to allow a patient to access their electronic health record using whatever app the patient chooses. There are no real protections that those app developers and sponsors will have security and privacy protections outside of HIPAA for the reuse of that data once the patient authorizes that the app have access to his or her electronic health record.
- Patients are now able to upload data that they have generated and obtained through consumer genetic testing. Some health care providers, for example, allow patients to upload their entire report from companies like 23andMe; and the Department's All of Us Research Program permits individuals to authorize that information be added to their health records.
- HIPAA is built around the notion of stewardship and trusted intermediaries. How do we protect national priority uses like public health uses of data that HIPAA was designed to allow and make sure they do not fall by the wayside?
- How will apps and the Internet of Things be meshed under pressure from providers that may have to provide a heightened level of protection that is kind of locked into software in a block chain system? How will that mesh with this old system of HIPAA?
- Some organizations sell data for research purposes and information subjects have not necessarily given informed consent for these uses and disclosures. Further, there are little or no protections against re-disclosure.
- The concept of de-identification is becoming or has become obsolete.
- There are some evolving expectations of privacy given the sheer volume of social media and the general population's willingness to share an enormous amount of information.
- There is a new privacy landscape, including the California Consumer Privacy Act (CCPA),<sup>3</sup> General Data Protection Regulation (GDPR),<sup>4</sup> HIPAA regulations, and state laws. Just like GDPR, CCPA has the ability to remove information, which in a health care organization we do not want to remove their medical information. That is the

---

<sup>3</sup> The [California Consumer Privacy Act](#), is a bill that strengthens privacy rights and consumer protection for residents of California and signed into law on June 28, 2018.

<sup>4</sup> The [General Data Protection Regulation](#) is a law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. It was implemented on May 25, 2018.

biggest challenge that health care organizations in places like California are facing today.

## **Themes**

The following themes developed out of these discussions:

### **1. Health Information Beyond HIPAA**

The US has two distinct health information privacy worlds: one world is regulated by HIPAA and administered by covered entities and business associates; the other world involves a growing range of uses by non-covered entities in the private sphere — consumers, technology companies, or sectors other than health — that are exempt from HIPAA. That world is largely unregulated.

### **2. Technologies**

Technologies for capturing, moving, and analyzing health information such as personal health devices, the Internet of Things, and new analytic techniques that are not covered by HIPAA, are not required to adhere to common minimal regulatory or voluntary privacy guidelines.

### **3. Consumers**

Consumers are asserting their information rights as awareness increases about the breadth of ways personal information, including health information, is being repurposed.

### **4. Lagging Policy**

Existing mechanisms for developing policy on privacy protections cannot match the pace of change.

### **5. Patchwork Approach**

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

### **6. Importance of Private Sector**

Voluntary stewardship and governance practices can help to safeguard privacy, but there is little incentive for organizations that handle health information to take the extra steps necessary to go beyond what is strictly required.



## **Naming the Framework**

Meeting participants discussed the guiding principles that were laid out in the 2007 framework, and there was deliberation around using the word “stewardship” versus “governance.” A suggestion was made instead to use “guiding principles for use and protection of health data” as a working title.

Additional discussion was given to individuals’ rights, and whether to use the phrase “maintain” or “strengthen” individual’s health information privacy or “individual’s rights regarding...” There was discussion around setting the context as legally enforceable rights, and others who would not limit the content to rights.

## **Guiding Principles for Use and Protection of Data**

Members and invited participants identified a range of principles for use and protection of data that should be considered in designing a contemporary framework. Areas of principles discussed include:

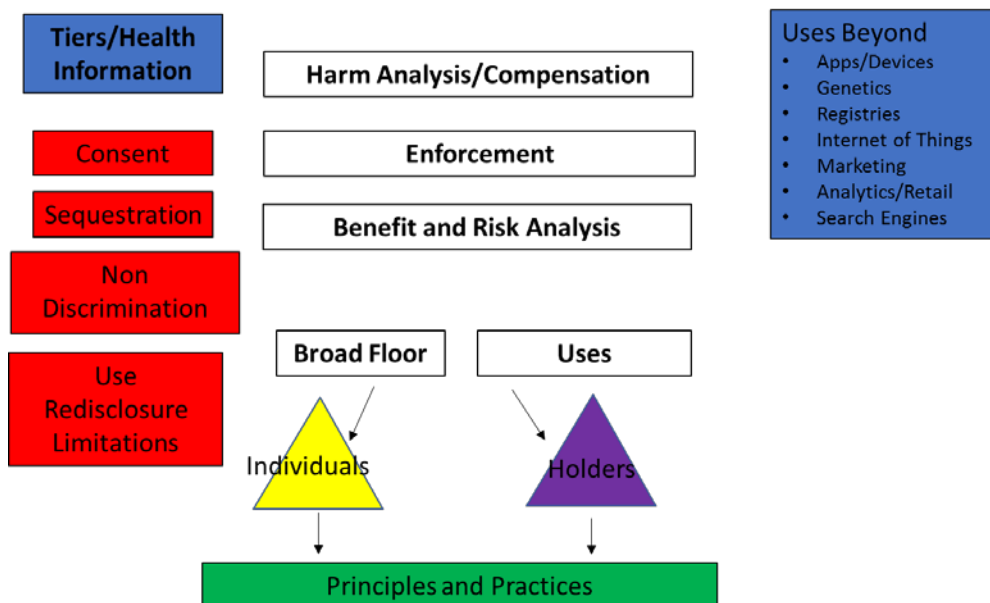
- Protections increase health equity (e.g., privacy and security, better use of data, better surveillance, health promotion)
- Consumers understand how to exercise their information rights and how information is used
- Data holders disclose what information they hold, how it is used, and shared (transparency)
- Purpose specification, collection, and use limitation
- Unconsented uses and disclosures are limited and clearly specified
- Consent requirements for disclosure are meaningful and understandable
- Collection of data as granular as possible, but more protection as data gets more granular
- Data is interoperable, protected at rest and in motion
- Individuals have the ability to exercise control over downstream uses for data not included in original consent
- Mechanisms for redress and mitigation of risk of harm
- Individuals have the ability to sequester and segment data for uses
- Information should be collected in the least identifiable form consistent with the use
- Incorporate ethical analysis
- Incorporate privacy by design in technology (e.g., Privacy Impact Assessment and risk mitigation)
- Privacy choices attach to the data, not the custodian
- Provenance is attached to data
- Innovation should be supported

## Guiding Principles and Model

In transitioning from principles to developing model assumptions, the group focused first on the role of private sector action opportunities. The group discussed that private sector actions are a combination of improved risk avoidance procedures, practices, standards and contracting. There was consensus that any useful framework for improving the protection of data beyond HIPAA has to apply to government and nongovernmental, public/private, commercial, non-profit. It has to be comprehensive.

Following discussion, the model was reimagined as follows:

## Beyond HIPAA and Beyond Health



The model looks at a broad floor of protection for personally identifiable information, with three ways to envision this: protections at the individual level, protections on use, and protections or some mechanisms for data holders.

The group's insight was that HIPAA excels at the intersection of data holders, covered entities, business associates, and specific uses, treatment, payment and healthcare operations and the other uses that were discussed.

Added to this was the notion of strengthening protective levers for individuals. A broad floor of protections for personally identifiable information that needs to include some kind of use based consent or authorization process, sequestration, segmentation. The group agreed that protections should follow the data.

At the top of the model, a title was added, "Beyond HIPAA and Beyond Health," because "Health" gets at different combination of uses and users that sit on top of that.

It was acknowledged that the model needs a risk model with regard to uses, and some way of identifying risks of harm. Enforcement mechanisms and redress compensation is for harmed individuals or organizations, including nondiscrimination.

The group also discussed tiers of health information.

It was suggested that there are some categories of people that need greater protection, for example a disease that stigmatizes.

Day One adjourned with an opportunity for public comment. No comments were offered or submitted electronically.

---

## **DAY TWO**

The focus for this second day of the meeting was on developing the report.

### **Draft Report Outline**

The group revisited the emerging model against the guiding principles, and began in-depth discussions outlining the report which they agreed would include:

#### Health Information Definitions

- What is health information?
- Who owns information?
- What are the rights of individuals?
- What are the rights of data holders?
- What are remediations for harm?
- Public and Private Sector Actions

### **Timeline**

The group scoped out a timeline for finishing the report and recommendations. The Subcommittee chair laid out a schedule for biweekly meetings, with the goal of presenting for deliberation the draft report and letter with recommendations to the HHS Secretary to the NCVHS Full Committee Meeting on June 5-6, 2019, at the Humphrey Building in Washington, DC.

The meeting was adjourned.

## **Appendix A**

### **NCVHS Subcommittee on Privacy, Confidentiality and Security**

#### **Subcommittee Chair**

**Linda L. Kloss, MA**

President  
Kloss Strategic Advisors, Ltd.  
1101 Baywood Drive  
Vero Beach, FL 32963

#### **Subcommittee Members**

**Jacki Monson, JD**

Vice President  
Privacy & Information Security Officer  
Sutter Health  
2200 River Plaza Drive  
Sacramento, CA 95833

**Nicholas L. Coussoule**

Senior Vice President  
BlueCross BlueShield of Tennessee  
1 Cameron Hill Circle  
Chattanooga, TN 37402

**Vickie M. Mays, PhD, MSPH**

Professor and Director  
UCLA Department of Psychology & Health Services  
405 Hilgard Avenue  
1285 Franz Hall, Box 951563  
Los Angeles, CA 90095-1563

#### **Other Members of the National Committee on Vital and Health Statistics in Attendance**

#### **NCVHS Chair**

**William W. Stead, MD**

Chief Strategy Officer  
McKesson Foundation Professor of Biomedical Informatics  
Professor of Medicine  
Vanderbilt University Medical Center

1161 21st Avenue South  
D3300 Medical Center North  
Nashville, TN 37232-2104

**Alexandra (Alix) Goss**

Vice President and Senior Consultant  
Imprado / DynaVet Solutions  
3915A N. Front Street  
Harrisburg, PA 17110

**Debra Strickland, MS**

Wallingford, CT 06492

**Richard W. Landen, MPH, MBA**

Bonita Springs, FL 34136

**Lead Staff to the Subcommittee on Privacy, Confidentiality and Security**

**Rachel Seeger, MA, MPA**

Senior Advisor, Public Affairs and Outreach  
HHS Office for Civil Rights  
200 Independence Avenue, NW  
Washington, DC 20201  
Phone: 202-774-3068  
Email: [rachel.seeger@hhs.gov](mailto:rachel.seeger@hhs.gov)

## **Staff to the Subcommittee on Privacy, Confidentiality and Security**

### **Maya Bernstein, JD**

Privacy Advocate ASPE/OSDP  
Department of Health and Human Services  
200 Independence Avenue, NW  
Washington, DC 20201  
Phone: 202-690-5896  
Email: [maya.bernstein@hhs.gov](mailto:maya.bernstein@hhs.gov)

### **Amy Chapper, JD**

Technical Advisor Privacy Rights & Protection Staff  
Center for Beneficiary Choices  
Centers for Medicare & Medicaid Services, DHHS  
7500 Security Boulevard, Mailstop S1-05-06  
Baltimore, Maryland 21244-1850  
Phone: 410-786-0367  
E-mail: [amy.chapper@cms.hhs.gov](mailto:amy.chapper@cms.hhs.gov)

### **Natalie Gonzalez, JD, LLM, CDC**

Public Health Analyst  
Office of Science Integrity  
Office of the Associate Director for Science (OADS), CDC, DHHS  
Clifton Building 21  
Atlanta, GA 30329  
Phone: 404-639-7559  
Email: [hv7@cdc.gov](mailto:hv7@cdc.gov)

### **Kathryn Marchesini, JD**

Privacy Branch Chief  
Office of the National Coordinator for Health Information Technology, DHHS  
200 Independence Avenue, SW  
Washington, DC 20201  
Phone: 202-690-3948  
Email: [kathryn.marchesini@hhs.gov](mailto:kathryn.marchesini@hhs.gov)

## Appendix B

### NCVHS Subcommittee on Privacy, Confidentiality and Security Invited Experts

*March 21-22, 2019*

**Barbara Evans Ph.D., J.D.**

**Mary Ann & Lawrence E. Faust Professor of Law  
Director of the Center for Biotechnology & Law  
University of Houston Law Center**

Barbara Evans is the Mary Ann & Lawrence E. Faust Professor of Law and Director of the Center for Biotechnology & Law at the University of Houston Law Center, a member institution of the Texas Medical Center. She holds a joint appointment as Professor of Electrical and Computer Engineering at the UH Cullen College of Engineering. Her current research interests include FDA regulation of machine-learning clinical and patient decision support software and gene sequencing and editing technologies; health data privacy and access; genomic civil rights; and citizen science and citizen-led bioethics standard-setting. She was named a Greenwall Foundation Faculty Scholar in Bioethics for 2010-2013 and is an elected member of the American Law Institute. Her recent activities have included service on the U.S. National Academies' Committee on Future Biotechnology Products; the Institute of Medicine's Committee on Accessible and Affordable Hearing Health Care for Adults; the U.S. Food and Drug Administration's Sentinel System Privacy Panel, Patient Engagement Working Group, and National Evaluation System for Health Technologies Planning Board; and the U.S. National Committee for Vital and Health Statistics. She holds an electrical engineering degree from the University of Texas at Austin, an M.S. and Ph.D. in Earth Sciences from Stanford University, a J.D. from Yale Law School, and she completed a postdoctoral fellowship in clinical ethics at the University of Texas M.D. Anderson Cancer Center.

**Leslie Pickering Francis. Ph.D., J.D.**

**Alfred C. Emery professor of law  
Professor of Philosophy  
University of Utah**

Leslie P. Francis, Ph.D., J.D., holds joint appointments as Alfred C. Emery professor of law and professor of philosophy, and adjunct appointments in Family and Preventive Medicine (in the Division of Public Health), Internal Medicine (in the Division of Medical Ethics), and Political Science, at the University of Utah. She was appointed to the rank of Distinguished Professor in 2009 and became director of the University of Utah Center for Law and Biomedical Sciences in 2015. Professor Francis was President of the Pacific Division of the American Philosophical Association in 2015-2016. She currently serves as the elected Secretary-General of the International Society for Philosophy of Law and Social Philosophy and as a member of the Ethics Committee of the American Society for Reproductive Medicine. She is past co-chair of the Privacy, Confidentiality, and Security Subcommittee of the National Committee on Vital and Health Statistics, where she currently serves as a member of the Working Group on Data Access and Use. Professor Francis also has been a member of the Medicare Coverage Advisory Committee and of the American Bar Association's Commission on Law and Aging.

Professor Francis's books include *The Patient as Victim and Vector: Ethics and Infectious Disease* (co-authored with Battin, Jacobson, & Smith; Oxford University Press 2010); *Privacy: What Everyone Needs to Know* (co-authored with John Francis; Oxford, forthcoming June 2017); and *Sustaining Surveillance: the Ethics and Politics*

of Public Health Data Use (co-authored with John Francis; forthcoming Springer 2018). She edited the Oxford Handbook of Reproductive Ethics (Oxford, January 2017) and is the author of many papers in the areas of disability law and ethics, privacy and data use, justice, and bioethics.

**Melissa Goldstein, J.D.**

**Associate Professor**

**Milken Institute School of Public Health**

**George Washington University**

Melissa M. Goldstein, J.D., is an Associate Professor in the Department of Health Policy and Management at the Milken Institute School of Public Health at the George Washington University, where she teaches courses in bioethics (including genomics, reproductive ethics, end-of-life, and research ethics issues), health information technology policy, and public health law and conducts research on health information privacy and the legal and policy aspects of health information technology. Professor Goldstein is a former director of the Markle Foundation's health program, where she managed the policy subcommittee of Connecting for Health and other policy aspects of the foundation's work in health information technology. Ms. Goldstein has also worked as a legal consultant to President Clinton's National Bioethics Advisory Commission, a senior litigation associate at Skadden, Arps, Slate, Meagher, and Flom, LLP, and a White House Fellow and domestic policy advisor to Vice President Al Gore.

Professor Goldstein graduated Phi Beta Kappa from the University of Virginia, received her law degree from Yale Law School, and completed a post-doctoral fellowship in bioethics and health policy at Johns Hopkins and Georgetown Universities. She has served as a member of GW's IRB and hospital ethics committee and speaks frequently on issues in bioethics, health policy, health information privacy, and health information technology. Ms. Goldstein's recent research and writings have focused on privacy and security issues in health information exchange and the use of big data, as well as the effects of health information technology on the physician-patient relationship and patient engagement. During the 2010-2011 academic year, Professor Goldstein served as a senior advisor to the Chief Privacy Officer in the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Most recently, Professor Goldstein served as the Assistant Director for Bioethics and Privacy in the White House Office of Science and Technology Policy during the final year of the Obama Administration.

**Sallie Milam, J.D.**

**Deputy Director**

**Network for Public Health Law, Mid-States Region**

Sallie Milam, JD, CIPP/US/G, is a Deputy Director with the Network for Public Health Law, Mid-States Region. The Network for Public Health Law promotes and supports the use of law to protect the public's health by providing direct technical assistance; developing and providing training, materials, and practical tools; and connecting individuals with one other to build a public health law community. Ms. Milam's work focuses on navigating law to share data within and across sectors to address health inequities. She has practiced law for over 25 years primarily in the health, HIPAA, and general privacy areas and has extensive experience working with state agencies and their data. From 2003 to 2018, she served as West Virginia's Chief Privacy Officer and led the Executive Branch's Privacy Program. Previously, Ms. Milam facilitated data sharing through her service as the West Virginia Health Care Authority's Privacy Officer and as HIPAA Senior Legal Counsel, where she led HIPAA privacy implementation across the West Virginia Executive Branch. She was the first Executive Director of the West Virginia Health Information Network, which is West Virginia's statewide health information exchange, and was West Virginia's Project Director for its Nationwide Health Information Network contract.

**Mark A. Rothstein, J.D.**

**Herbert F. Boehl Chair of Law and Medicine**



**Director, Institute for Bioethics, Health Policy and Law  
University of Louisville School of Medicine**

Professor Rothstein holds joint appointments at the University of Louisville in the Brandeis School of Law and the School of Medicine. He holds the Herbert F. Boehl Chair of Law and Medicine and is the Founding Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. He joined the University of Louisville faculty in 2001. Professor Rothstein has concentrated his research on bioethics, genetics, health privacy, public health law, and employment law. From 1999-2008 he served as Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital Health Statistics, the statutory advisory committee to the Secretary of Health and Human Service on health information policy. He is past president of the American Society of Law, Medicine and Ethics. He serves as Public Health Ethics Editor for the American Journal of Public Health, and he writes a regular column on Bioethics for the Journal of Law, Medicine & Ethics. Additionally Mr. Rothstein has authored 19 books and over 250 articles on his areas of research. He holds a Bachelor's degree from the University of Pittsburgh and earned a J.D. at Georgetown University.



## Appendix C

### **Audience and WebEx Attendees**

Lana Moriarty, ONC

Penelope Hughes, ONC

Sharon Franchock, BCBSM

Marilyn Zigmund Luke, AHIP

Susan Queen, NCHS

Susan Dardine

Natalie Gonzalez

Rachel Nelson

Meryl Bloomrosen

Penelope Hughes

Cynthia Bush

Sharon Franchock

Heather McClane

I hereby certify that, to the best of my knowledge, the foregoing summary of minutes is accurate and complete.

[REDACTED]

Chair

06/06/2019

Date