CONFIDENTIALITY COALITION

GENERAL COMMITTEE MEETING

Thursday, November 21, 2019
3:00 PM to 4:00 PM

Healthcare Leadership Council
750 9th Street, NW, Suite 500 Washington, D.C. 20001
Conference Line: 857-232-0157, **Code:** 30-40-73

1. **Welcome and Introductions**

2. **Guest Speaker: Elyssa Malin** **Attachment 1**
   Policy Advisor, Office of Senator Amy Klobuchar
   Topic: *Health Information Privacy Policy*

3. **Privacy Legislation Framework** *(Senate Ranking Members)* **Attachment 2**

4. **Beyond HIPAA Privacy Principles** – *FINAL* **Attachment 3**

5. **2020 Agenda**

Privacy and Data Protection Framework

Our lives are shaped by technology and data collection more than ever before. Yet the basic legal frameworks to protect our privacy have not evolved—or been updated—to meet this new reality. As a result, corporations and other entities have greater and more direct access to consumers' private and sensitive information, enabling them to amass vast amounts of data, and in some cases place consumers at risk of harm.

We believe that a comprehensive federal privacy and data security law is essential to hold institutions accountable, restore consumer trust, and protect our privacy.

We have developed a set of core principles that should be included in any comprehensive data protection legislation. Under our framework, consumers would control their personal information, and corporations, non-profits, and political entities would be held to higher standards for when and how they collect, use, share, and protect our data. Nothing in this framework should be interpreted to change or displace existing privacy laws, or privacy laws scheduled to go into effect.

Our privacy principles will:

ESTABLISH DATA SAFEGUARDS

- **Minimization:** Collection of data must be minimized so that it is narrowly tailored to its authorized use. We must establish strict limits around the use, extrapolation, and retention of certain data, especially data relating to biometrics, race, sexual orientation, children, health, or finances.
- **Abuse Prevention:** Harmful, deceptive, and abusive collection and use of data must be prohibited. Standards must ensure that data is only processed in a transparent manner that meets consumers' expectations and is free from unlawful manipulation.
- **Sharing Limits:** To ensure that consumers are protected throughout the marketplace, we must establish clear rules to limit data sharing with service providers and third parties to that which is needed to carry out the express purposes expected and authorized by consumers.
- **Security:** We must provide greater accountability and higher standards over the way organizations retain and secure data.

INVIGORATE COMPETITION

- **Market Power Checks:** Consumers must have the ability to prevent their data from being commingled across separate businesses within an enterprise, and to ensure that privacy protections, including restrictions on commingling or repurposing, apply to data obtained through mergers, acquisitions, or bankruptcies.
- **Data Portability:** To boost choice in the marketplace and level the playing field for entrepreneurs, consumers must be empowered to take their data to the company of their preference.

STRENGTHEN CONSUMER AND CIVIL RIGHTS

- **Individual Consumer Rights:** Consumers must have the right to control their data, including the right to know, access, delete, correct, and restrict the transfer and retention of their records. Organizations that collect and store our data must be required to provide clear, concise disclosure of and justification for their privacy practices, and supply consumers with meaningful options to access products or services without sacrificing their privacy. We must also have heightened protections and tools in place, like a do-not-track right, to prevent consumers from being targeted online and tracked across websites, and to protect children and teens.

- **Civil Rights Protections:** Computer-based decisions that result in illegal bias or discrimination are unacceptable. Consumers must have transparency into black box algorithmic decisions that may result in bias or discrimination, and the ability to challenge such decisions. Entities that process consumer data in automated systems must be required to review such algorithms in order to prevent discriminatory impact. Enforcers must also be fully equipped to protect against unlawful discrimination in addition to voter targeting and suppression.

IMPOSE REAL ACCOUNTABILITY

- **Corporate Accountability:** Accountability mechanisms must shift the responsibility and liability of protecting privacy from consumers, who are overly burdened with understanding complicated, take-it-or-leave-it privacy policies, to the entities that hold their data and their senior corporate executives. Consumers must be able to trust that organizations secure their data, use it ethically, and do not use it to consumers' detriment. Increased Chief Executive Officer (CEO) accountability, whistleblower rights, and consumer redress mechanisms are just a few of the many tools that must be provided to ensure corporations are held to account.

- **Federal Enforcement and Rulemaking:** Enforcement of privacy rights must serve as a serious deterrent, not just an acceptable cost of doing business. Among other changes, federal enforcers must be able to seek significant civil fines and criminal penalties, where possible, in the first instance of privacy and data security violations. Federal enforcers must also have streamlined rulemaking authority to ensure that the strong legal protections imposed by this law can evolve and adapt to new technologies, and equipped with adequate staff and resources to implement these protections.

- **State and Private Remedies:** Federal enforcement must be complemented by state enforcement of federal protections and private rights of action, as is common in existing privacy laws and other fields. The private right of action must be meaningful, and not one that can be overridden by a mandatory arbitration clause buried within onerous and lengthy terms and conditions.

Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.

    a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.

    b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.

2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:

    a. Should not conflict with HIPAA,
    b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
    c. Should align with HIPAA's definitions of health information, and
    d. Should adopt a risk-based approach like HIPAA.

3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.

4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.

6. Individuals must provide authorization for entities outside of HIPAA to collect individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.

7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.

8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.