June 28, 2022

Hacking Healthcare

TLP White

This week, Hacking Healthcare's "Yes, This Is Still a Thing" department focuses on a new bill attempting to create a "comprehensive" federal data privacy law for the United States. Beyond providing some context for the bill, we will examine who would be affected if the bill passed, what types of data are covered, what types of security and privacy requirements are present, how the bill would interact with existing healthcare-focused regulation and legislation, and what the prospects are of the bill being signed into law.

Welcome back to *Hacking Healthcare*.

1. The American Data Privacy and Protection Act

While comprehensive data privacy laws have slowly begun to proliferate over the years in other countries and regions, highlighted by the E.U.'s *General Data Protection Regulation* (GDPR), the United States has failed to advance an overarching federal law. Despite its lead role in developing standards and best practices in the IT/security space, attempts at legislating data privacy have continually run into seemingly insurmountable hurdles. While the recently introduced *American Data Privacy and Protection Act* (ADPPA) is far from landing on President Biden's desk, it represents the best chance of a federal privacy law passing in some time. The bill's current language would have an enormous effect, including on the healthcare sector.

The significance of the ADPPA's bipartisan and bicameral support from key members of Congress cannot be overstated. However, the current text of the bill as introduced has little chance of progressing, and it's understood that numerous sections remain contentious for both congressional Democrats and Republicans. With the understanding that some sections may be significantly revised, and many more slightly so, here are some of the provisions and issues that those in the healthcare sector should be aware of.

<u>Who Is a "Covered Entity" and What Is "Covered Data"?</u>

The current bill text defines “Covered Entities” as “any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data; and is subject to the FTC Act; or is a Common Carrier; or is a non-profit.”[1] The bill would also cover “any entity or person that controls, is controlled by, or is under common control with another covered entity,” as well as outlining requirements for service providers.[2] The only listed exclusions are government entities.[3]

As for “Covered Data,” the bill defines it as “information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual and may include derived data and unique identifiers.”[4] Exclusions are extended to de-identified data, employee data, publicly available information, and “inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.” All of these terms are defined within the bill’s text.

Notably, there is a further distinction within covered data that may be especially applicable to many healthcare sector organizations. “Sensitive Data” includes a long list of specific data types such as biometric data, genetic data, and “any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.”[5] Such data has additional restrictions placed upon it.

Section 103 Privacy by Design

Section 103 of the bill relates to policies, practices, and procedures that would be required for covered entities and service providers. This section states that these entities will have to “establish, implement, and maintain reasonable policies, practices, and procedures regarding the collection, processing, and transfer of covered data.”[6] These polices, practices, and procedures should take into account numerous factors such as the size of the covered entity, the sensitivity of the data in question, the volume of data, as well as the cost of implementation in relation to risk. The FTC would be required to provide guidance within one year of the ADPPA’s enactment to help define “reasonable policies, practices, and procedures.”[7]

Section 208 Data Security and Protection of Covered Data

Similar to Section 103, Section 208 introduces requirements to “establish, implement and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.” The similarities to Section 103 extend to the consideration of factors such as size of the covered entity, sensitivity of the data in question, and volume of data. However, Section 208 adds that organizations shall also consider “the current state of the art in administrative, technical, and physical safeguards for protecting such covered data."[8]

This section also outlines seven specific data security practice requirements that are to be included as a bare minimum. These include assessing vulnerabilities, taking preventive and corrective actions, evaluating those preventive and corrective actions, proper information retention and disposal activities, adequate employee training, the designation of personnel to maintain and implement data security practices, and implementing incident response procedures.

Preemption and Applicability of Other Information Security Laws

Many organizations already have legal and regulatory requirements that cover areas mentioned above, and the bill's authors and co-sponsors acknowledge that finding a balance between preempting and coexisting alongside existing state and federal laws and regulations is necessary. For healthcare organizations in particular, Sections 208 and 404 outline how the ADPPA's data privacy and security provisions integrate with the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH Act):[9]

- Section 208 – The section contains language stating that covered entities that are required to comply with the HITECH Act, and that are deemed to be in compliance with the information security requirements of that Act by its enforcement authority, "shall be deemed in compliance with the requirements of section 208 with respect to any data covered by such information security requirements."

- Section 404 – Within this section, which outlines the relationship of the bill to federal and state law, there is language that outlines how a covered entity that is required to comply with the HITECH Act and/or the regulations promulgated pursuant to Section 264(c) of HIPAA, and that is deemed to be in compliance with the data privacy requirements of such regulations, will be deemed to be in compliance with the related requirements of the ADPPA.

- Section 404 – Additionally, Section 404 contains language stating that a covered entity that is required to comply with the HITECH Act and/or the regulations promulgated pursuant to Section 264(c) of HIPAA, "and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable) shall be deemed to be in compliance with the requirements of section 208 with respect to data subject to the requirements of such regulations."

> To be clear, this is not a comprehensive list of all state and federal exemptions and preemptions currently in the bill. In addition to the HITECH Act and HIPAA, the current text outlines numerous categories of other types of state laws and regulations that are not meant to be preempted by the ADPPA. One such exception relates to "laws that address health information, medical information, medical records, HIV status, or HIV testing."[10] Keep in mind that the language in this section may see significant changes should the bill advance.
>
> *Action & Analysis*

Congress

Tuesday, June 28th:
- No relevant hearings

Wednesday, June 29th:
- House of Representatives - Committee on Science, Space, and Technology - Subcommittee on Investigations and Oversight: Hearing: Privacy in the Age of Biometrics

Thursday, June 30th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness, and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and

Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[1] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[2] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[3] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[4] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[5] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[6] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[7] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[8] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[9] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[10] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf