July 13, 2022

TLP White

This week, Hacking Healthcare begins by exploring what the Biden administration's new Executive Order (EO), *Protecting Access to Reproductive Health Care Services,* may mean for entities subject to HIPAA. Next, we briefly cover why the National Institute of Standards and Technology's (NIST) announcement of post-quantum cryptographic algorithms will be important to the healthcare sector.

Welcome back to *Hacking Healthcare*.

1. **Biden Administration Addresses Health Data Privacy in Light of *Roe* Decision**

   The Supreme Court of the United States' (SCOTUS) decision to overturn *Roe v. Wade* has created considerable controversy. In a bid to help minimize the effects of the SCOTUS decision, and to provide some reassurances that his administration is committed to pushing Congress to restore protections as federal law, President Biden signed an EO and congressional lawmakers have been talking up legislation. While the right to access abortion is the heart of the issue, overturning *Roe v. Wade* has also led to increased scrutiny on the privacy of healthcare data. This aspect of the post-*Roe* environment may become heightened in the coming months.

   In response to the SOCTUS decision, President Biden signed an EO and published a Fact Sheet on July 8th.[1] The *Order Protecting Access to Reproductive Health Care Services* broadly covers four areas that are outlined in the White House's Fact Sheet:[2]

   - Safeguarding access to reproductive health care services, including abortion and contraception;
   - Protecting the privacy of patients and their access to accurate information;
   - Promoting the safety and security of patients, providers, and clinics;
   - Coordinating the implementation of federal efforts to protect reproductive rights and access to health care.

   The second bullet, protecting the privacy of patients and their access to accurate information, extends to "addressing the transfer and sales of sensitive health-related

data, combatting digital surveillance related to reproductive health care services, and protecting people seeking reproductive health care from inaccurate information, fraudulent schemes, or deceptive practices."[3] Within this section, the White House has outlined two general lines of effort: (1) Protect Consumers from Privacy Violations and Fraudulent and Deceptive Practices, and (2) Protect Sensitive Health Information.

The first line of effort includes asking the "Federal Trade Commission to consider taking steps to protect consumers' privacy when seeking information about and provision of reproductive health care services," while also directing "the Secretary of HHS, in consultation with the Attorney General and Chair of the FTC, to consider options to address deceptive or fraudulent practices, including online, and protect access to accurate information."[4]

However, the more pertinent action item is the protection of sensitive health information. The White House Fact Sheet announced that the Department of Health and Human Services (HHS) "will consider additional actions, including under the Health Insurance Portability and Accountability Act (HIPAA), to better protect sensitive information related to reproductive health care."[5] This includes directing HHS's Office for Civil Rights to take steps to "ensure patient privacy and nondiscrimination of patients, as well as providers who provide reproductive health care."[6]

This second line of effort has already resulted in new HIPAA Privacy Rule guidance being issued by HHS.[7] The guidance plainly reiterates to individuals and healthcare organizations what the HIPAA Privacy Rules require, such as a breakdown of disclosures required by law and disclosures for law enforcement purposes. It also outlines how individuals can file a privacy compliant should they feel their privacy rights have been violated.

Action & Analysis
Membership required

2. NIST Announces Quantum-Resistant Cryptographic Algorithms

On July 5th, the National Institute of Standards and Technology (NIST) announced four quantum-resistant cryptographic algorithms to be part of the first wave of tools "designed to withstand the assault of a future quantum computer."[8] These four will become part of the NIST post-quantum cryptographic standard and will likely become leading candidates for global adoption in the near term, as organizations begin to think about preparing for the day when current cryptographic standards are no longer capable of protecting data from emerging technologies.

The announcement last week is the product of a six-year effort begun by NIST in 2016 "to help future-proof electronic information."[9] Specifically, the effort was meant to

address the potential threat that quantum computers could pose to current encryption algorithms. While the initial project acknowledged that practical quantum computing is some ways off, significant advances since then in the development of quantum computers have underscored the need to develop and test quantum-resistant cryptographic algorithms.

The four algorithms chosen are designed to be used for either general encryption or for digital signatures, and more algorithms are likely on the way. NIST is currently evaluating four other candidates for possible inclusion in the eventual NIST post-quantum cryptography standard that is planned for release by 2024.[10]

Action & Analysis
Membership required

Congress

Tuesday, July 12th:
- No relevant hearings

Wednesday, July 13th:
- No relevant hearings

Thursday, July 14th:
- 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://www.whitehouse.gov/briefing-room/presidential-actions/2022/07/08/executive-order-on-protecting-access-to-reproductive-healthcare-services/

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

[6] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

[7] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

[8] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[9] https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information

[10] https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline