GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

January 2021

Cheers to Heightened Health (Privacy) in 2021

Much changed in the privacy law landscape in 2020, including a heightened focus on the use and disclosure of health information. As 2021 gets underway, businesses should be aware of the key legislative and regulatory changes in health data privacy that were teed up at the close of 2020, and which may now or soon affect them.

HIPAA Proposed Rulemaking

The Office for Civil Rights at the U.S. Department of Health and Human Services (HHS) released proposed changes to the HIPAA Privacy Rule on Dec. 10, 2020. The proposed changes focus on strengthening individuals' access to their health information, facilitating greater caregiver involvement in the care for individuals, and improving access to protected health information (PHI) during emergencies or health crises. There are five primary things to consider in the proposal:

1. HIPAA-covered entities' current 30-day required response time to give individuals access to their PHI would be cut to 15 days.

2. The modifications would create a mechanism for individuals to direct sharing of their PHI among covered health care providers and health plans.

3. The proposed changes aim to strengthen patient access to their PHI by permitting individuals to inspect their PHI in-person, including taking notes or using other personal devices to view and capture images of their records.

4. The proposed rule would require specifications for when electronic PHI must be provided to the individual at no charge.

5. The changes would require HIPAA-covered entities to post estimated fee schedules on their websites for both PHI access and disclosures with an individual's valid authorization as well as provide individualized estimates of fees for an individual's request for copies of PHI.

Public comments will be due 60 days after publication of the proposal in the Federal Register.

California's Consumer Privacy Act (CCPA)

While the CCPA excludes PHI processed under HIPAA (and medical information protected by the California Confidentiality of Medical Information Act), health care and life sciences companies may nevertheless find themselves subject to the law due to data processing activities outside of their health privacy compliance programs, such as:

- Non-PHI health data, including:
  - health and wellness information collected from an individual (wearable devices and mobile apps);
  - employment records (especially in light of myriad COVID-19 employer-testing programs);
- De-identified PHI, i.e., data de-identified under HIPAA that may still be personal information under the CCPA due to it being capable of re-identification; and
- Inferences drawn from PHI that can be reasonably linked to an individual.

On Sept. 25, 2020, the California governor signed into law AB 713, which amends the CCPA's HIPAA exception in a number of ways. AB 713 makes an exception for "business associates" under HIPAA; clarifies that the CCPA does not apply to data that was de-identified pursuant to HIPAA standards and derived from patient information originally collected by a HIPAA-regulated entity; expands the scope of the CCPA's health research exceptions to cover studies other than clinical trials; prohibits re-identification of de-identified patient information; and imposes new contracting and notice requirements for certain disclosures of de-identified patient information. AB 713 became operative immediately, except for the law's new contractual requirements that went into effect Jan. 1, 2021.

The health-related exceptions under the CCPA will still be carved out under the recently passed California Privacy Rights Act (CPRA). As such, health companies can get ahead of CPRA compliance by taking actions to comply with the CCPA and AB 713 now.

Health Information Blocking Rules Extended

In November 2020, the HHS Office of the National Coordinator for Health Information Technology (ONC) published an Interim Final Rule: Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency (Interim Final Rule) providing relief to entities working toward compliance with the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Rule), issued May 1, 2020. The Interim Final Rule provides regulated entities with "additional flexibilities" to implement the provisions of the ONC Rule including updated compliance dates. ONC explained that the extension is due to the COVID-19 public health emergency.

On Jan. 4, ONC released new resources and guidelines for requirements related to its upcoming information-blocking rules.

COVID-19 Vaccine Reporting

The Centers for Disease Control and Prevention is instructing states to sign data use agreements that commit them for the first time to sharing personal information related to COVID-19 vaccinations in existing state registries with the federal government. States normally collect this type of data themselves, but some are pushing back against giving it to federal authorities due to privacy and data use concerns, with Minnesota and Colorado, for example, saying they will only share de-identified data. Other states, such as New York, are refusing to sign or share the information at all.

Sen. Klobuchar Seeks Consumer Health Privacy Protections

Sen. Amy Klobuchar (D-Minn.) has asked HHS to provide more consumer privacy protection in response to new wearable health devices. On Dec. 11, 2020, Sen. Klobuchar sent a letter to HHS Secretary Alex Azar asking what HHS is doing to ensure such devices safeguard sensitive health information. In 2019, Klobuchar sponsored legislation with Sen. Lisa Murkowski (R-Alaska) to regulate tracking devices, health apps and home DNA testing kits. The Protecting Personal Health Data Act proposed that the HHS secretary create regulations for new direct-to-consumer health regulations not covered by existing laws.

FBI and HHS Release Ransomware Alert

On Nov. 2, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and HHS jointly released the Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (the Alert). The Alert provides extensive detail regarding the mechanism and indicators of Trickbot malware. Trickbot is used to deploy Ryuk ransomware, which has reportedly recently forced multiple hospitals across the country offline in a coordinated attack. The Alert includes best practices for health care providers to minimize risk and mitigate harm, including the following critically important practices:

1. Implement business continuity plans – or plans to continue essential functions through emergencies such as cyberattacks and to minimize service disruptions;

2. Maintain formal and informal training and security awareness programs, covering ransomware and phishing scams;

3. Patch system, software, and firmware as new patches are released;

4. Require regular password changing; and

5. Implement multi-factor authentication.

The Alert also includes some ransomware best practices, such as:

- Do not pay the ransom (payment does not guarantee that files will be recovered, and it emboldens cyber criminals);
- Regularly back up data and secure backup copies offline;
- Engage with CISA, FBI, and HHS for information-sharing, best practices, and other resources;

- Retain three copies of all critical data on at least two different types of media with at least one stored offline.

Click here to subscribe to Greenberg Traurig's Data Privacy Dish blog.

Author

This GT Alert was prepared by:

- Kate Black | +1 305.579.0500 | blackk@gtlaw.com