Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Privacy Versus Pandemic: Health Privacy Considerations in Response to COVID-19

March 25, 2020

As COVID-19 continues to spread, health care providers, health plans and employers are facing difficult privacy questions as they attempt to balance privacy concerns against the need to protect patients, employees and customers from potential infection. Determining how much information to share regarding individuals affected by COVID-19, and with whom, requires a fact-specific analysis under a patchwork of legal obligations, including those related to privacy, public health, and employment. This piece provides a framework for a course of action, highlighting key considerations and best practices, for those undertaking this complex analysis.

Evaluate Potentially Applicable Privacy Requirements

When faced with a situation involving COVID-19-related health information, as a first step, organizations should evaluate which state and federal privacy laws might apply as they make decisions on what they can or should share with others. The applicability of certain legal obligations will depend on a variety of factors, including the type of organization, the nature and scope of health information at issue, the context in which that information was received, the relationship between the COVID-19-affected individual and the organization, and the purpose of any contemplated disclosures.

Review Federal and State Privacy Law Through a COVID-19 Lens

The Health Insurance Portability and Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act of 2009, together with their implementing regulations (HIPAA), establishes the primary federal legal regime concerning health information privacy, but it does not apply in all situations.[1] At its core, the HIPAA privacy rule restricts the use and disclosure of individually identifiable health information (defined broadly to include demographic information) without authorization, subject to limited exceptions. Health plans, covered health care providers (such as hospitals, pharmacies and nursing homes), and health care clearinghouses are considered "covered entities" and are required to comply with HIPAA. Business associates of these covered entities, which create or receive HIPAA-protected information in the course of performing functions or services for them or on their behalf, are also subject to many of HIPAA's requirements. Covered entities and

Contact Information

If you have any questions concerning this alert, please contact:

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Mallory A. Jones
Associate
jonesm@akingump.com
Washington, D.C.
+1 202.887.4259

Caroline Dumesnil Kessler
Associate
ckessler@akingump.com
Washington, D.C.
+1 202.887.4514

business associates will need to evaluate their obligations relating to HIPAA carefully as they use and disclose health information in the COVID-19 crisis.

HIPAA may also extend to the employment setting. While HIPAA does not apply to employers acting in their capacity as employers, it does apply to many employer-sponsored group health plans. This means that HIPAA will generally not apply if an employee in the legal department, for example, informs his or her supervisor of a positive COVID-19 test. If, however, the employer learns about the positive test from someone in human resources who has responsibilities relating to the employer's self-insured group health plan and discovered the information while performing those responsibilities, HIPAA may apply and restrict use and disclosure of information regarding the positive COVID-19 test result. To the extent HIPAA applies, the employer may be prohibited from disclosing individually identifiable health information directly to other employees without a HIPAA-compliant authorization, unless required by law.

Beyond HIPAA, companies should evaluate whether state law might restrict their disclosure of employee health information related to COVID-19. For example, California's Confidentiality of Medical Information Act (CMIA) specifically prohibits employers from using, disclosing or knowingly permitting the disclosure of "medical information which the employer possesses pertaining to its employees without the patient having first signed an authorization . . . ," subject to limited exceptions.[2] Importantly, "medical information" in this context is limited to information "in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor," so employers should take a close look as to whether data may be in scope.[3]

Additionally, employers will have to consider labor and employment laws, like the Americans with Disabilities Act of 1990 (ADA) and the Occupational Safety and Health Act of 1970 (OSHA), as they deal with COVID-19 issues in the workplace. In a recent publication, for example, the U.S. Equal Employment Opportunity Commission clarified that employers are able, during a pandemic, to ask questions that might not otherwise be permissible under the ADA. For example, ADA-covered employers are permitted to ask employees who call in sick whether they have symptoms of the pandemic virus.[4] An employer may also take an employee's temperature before allowing them to enter the workplace.[5] It is important, however, that companies making medical inquiries as a tool to combat the spread of COVID-19 not allow privacy issues to fall by the wayside.

Privacy concerns extend beyond the health and employment settings, as some state privacy and data protection laws have broader reach. In some states, including Oregon, Washington, Illinois and Texas, an unauthorized disclosure of identifiable health information may be treated as a data breach under state breach notification laws and companies may be required to notify affected individuals and state authorities, depending on the specific facts and circumstances.[6] To avoid potentially giving rise to a reportable breach when keeping employees or customers informed about COVID-19-related health information, companies should generally limit the amount of information shared (excluding identifiers such as name and age of the affected individual, for example), should only provide health information when disclosure of such information is necessary or appropriate, and should have a strong grasp on what types of disclosures could trigger applicable state breach notification laws.

The issue becomes even more complicated for multinational companies, as foreign privacy laws may apply. Guidance from various data protection authorities in Europe and Asia has highlighted privacy concerns. Foreign governments are making adjustments to their privacy policies in an effort to grapple with the spread of the coronavirus.

Look for Public Health Exceptions to Privacy Laws Restricting the Use and Disclosure of Information

Importantly, exceptions—often narrowly crafted—are built into many privacy laws to afford organizations the ability to use and share otherwise protected information when an important public policy purpose prevails.

To the extent HIPAA applies, for example, two public policy exceptions may be particularly relevant to the COVID-19 crisis: the exception for uses and disclosures for public health activities, and the exception for uses and disclosures to avert a serious threat to health or safety.

HIPAA permits covered entities to disclose protected health information without the individual's authorization to public health authorities "authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability . . . ."[7] Similarly, covered entities may disclose protected health information to individuals "who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease"—but only if "the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation."[8] In a February bulletin, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) construed "as necessary in the conduct of a public health intervention or investigation" to include disclosures "necessary to prevent or control the spread of the disease."[9]

Covered entities are also permitted to make certain disclosures without individual authorization necessary to "prevent or lessen a serious and imminent threat to the health or safety of a person or the public," if consistent with state law and applicable standards of ethical conduct, subject to some limitations.[10] When this exception applies, a health care provider or other covered entity may disclose protected health information to anyone who is in a position to prevent or lesson the threat, including family, friends and law enforcement, without a patient's permission.[11]

In its February bulletin, OCR reminded covered entities how these and other HIPAA exceptions may be employed during the COVID-19 crisis.[12] Importantly, OCR cautioned that "for most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the 'minimum necessary' to accomplish the purpose."[13] OCR also reminded providers of the limitations on their ability to comment to the media without a patient's consent.[14] Furthermore, OCR released additional guidance on March 24, 2020, explaining the circumstances under which covered entities may disclose protected health information related to COVID-19 to law enforcement, paramedics, other first responders, and public health authorities without an individual's authorization.[15]

Beyond HIPAA, other state and federal privacy laws may contain public policy exceptions that could be relevant to disclosures related to COVID-19. Entities should

be sure to keep an eye out for these exceptions as they evaluate applicable legal requirements.

Consider Other Sources of Relevant Requirements

In addition to evaluating applicable privacy laws, companies should review relevant contracts, including employment agreements and collective bargaining agreements, for issues pertinent to the current crisis. Some contracts may make confidentiality or safety promises to employees or customers, for example, which would need to be evaluated. It is also possible that some agreements could mandate certain disclosures. Relevant promises could also be made through externally facing privacy policies or terms of use. Also, requirements pertinent to the use and disclosure of health information in the current crisis could potentially be found in sections of state codes focusing on public health and infectious diseases, separate from other privacy and data protection laws.

Pay Attention to New Developments

The past few years have been a time of rapid change in the privacy legal landscape, with comprehensive new privacy regimes taking hold in places like California and a broad range of changes to privacy, security and breach notification laws being considered or enacted from coast to coast. Change has become a constant in privacy law, and that should hold true as legislatures and regulators work to respond to the COVID-19 crisis.

For example, the federal government has shown some willingness to waive certain privacy requirements as health care providers tackle the treatment of an influx of COVID-19 patients. Regulators recently announced limited HIPAA enforcement flexibility waiving sanctions and penalties for hospitals that do not comply with certain listed HIPAA requirements, including regulations relating to a patient's right to request privacy restrictions or confidential communication, for a limited time.[16] This waiver is not universal. It applies only to hospitals—not to other covered entities—and only where the hospital has instituted and implemented a disaster protocol related to the officially declared public health emergency.[17] Regulators also announced a separate waiver intended to enable more providers to furnish health care services remotely through everyday communications technologies.[18]

On the HIPAA front, additional guidance may be forthcoming, either from HHS or Congress.[19] States may also take action to adapt their privacy and data protection laws to the demands of the COVID-19 crisis.

Plan for Privacy Issues Related to COVID-19

To reduce the risk of running afoul of health privacy laws in COVID-19 response efforts—and to keep related questions from causing confusion and delay—it is important for all companies to devote some time now to examining their internal and external policies and considering whether any adjustments are needed to address health privacy issues in the face of the current crisis.

Companies should consider developing and testing internal and external communication plans to have guiderails ready upon learning that an employee, customer or other individual affiliated with the organization has fallen ill with COVID-19 symptoms, has tested positive for COVID-19, has a confirmed direct exposure to

someone with a positive test, or has an exposure that is more removed or attenuated. The plan should contemplate the types of information that would (and would not) be shared under various scenarios, how it would be communicated, and to whom. Importantly, the plan should establish a clear protocol for engaging with public health officials. In most cases, employers should let state and federal health officials do the talking as much as possible, including tracking down individuals who may have been in contact with the affected employee.

In some cases, it may make sense for companies to seek consent for information disclosures relating to COVID-19 crisis, either *en masse* in advance or on a case-by-case basis as the need arises. This is particularly true where an employer is considering implementing some form of medical surveillance. Companies taking this approach would need to consider specific consent requirements under all potentially applicable laws. Some jurisdictions may be quite exacting (for example, CMIA, referenced above, requires consent to be in at least 14-point font or hand-written to be valid).[20]

Updates to privacy policies and procedures may also be warranted, especially for entities that are subject to HIPAA. For all companies, outward-facing privacy policies and terms of use should be reviewed to confirm that data practices remain accurately described, as some shifts may have occurred due to the pandemic. Internal privacy policies and procedures should be reviewed as well to ensure they reflect current practices and plans. This step will be particularly important for health care providers, as HIPAA policies and procedures should be evaluated to ensure they are not so restrictive as to hinder staff's access to information in a way that limits their ability to protect themselves and other patients from potential COVID-19 infection. The spread of COVID-19 has the potential to cause an overabundance of curiosity, and staff may be tempted to snoop in patient records without a legitimate need. Once policies and procedures are fine-tuned for the current crisis, personnel should be retrained, as feasible under the circumstances, to ensure expectations are clear.

And finally, all companies whose personnel are increasingly working from home should consider providing additional resources and training to help them do so securely.

With so many legal issues surrounding the spread of COVID-19, the landscape here could change quickly. Companies should both plan ahead and keep their ears to the ground for new developments so adjustments can be made as needed.

Additional resources on legal issues relating to COVID-19 can be found on Akin Gump's COVID-19 Resource Center.

[1] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1940; Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. 111-5, 123 Stat. 226; 45 C.F.R. Parts 160, 162, and 164.

[2] Cal. Civ. Code § 56 *et seq*.; *id.* § 56.20(c).

[3] *Id.* § 56.05(j).

[4] U.S. Equal Employment Opportunity Commission, What You Should Know About the ADA, the Rehabilitation Act, and COVID-19 (Mar. 2020), https://www.eeoc.gov/eeoc/newsroom/wysk/wysk_ada_rehabilitaion_act_coronavirus.cfm (last visited Mar. 21, 2020).

[5] *Id.*

[6] *See, e.g.*, Or. Rev. Stat. § 646A.602 (Oregon); Wash. Rev. Code § 19.255.005 (Washington); 815 Ill. Comp. Stat. 530/5 (Illinois); Tex. Bus. & Com. Code §§ 521.002, 521.053 (Texas).

[7] 45 C.F.R. § 164.512(b)(1)(i).

[8] *Id.* § 164.512(b)(1)(iv).

[9] U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), Bulletin: HIPAA Privacy and Novel Coronavirus at 3 (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.

[10] 45 C.F.R. § 164.512(j)(1)(i).

[11] *Id.* § 164.512(j)(1)(i)(B).

[12] HHS OCR, Bulletin: HIPAA Privacy and Novel Coronavirus at 3.

[13] *Id.* at 5.

[14] *Id.* at 4.

[15] HHS OCR, COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities (Mar. 2020), https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf.

[16] HHS, COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency (Mar. 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf (listing waived HIPAA provisions and emphasizing limitations: "The waiver became effective on March 15, 2020. When the Secretary issues such a waiver, it only applies: (1) in the emergency area identified in the public health emergency declaration; (2) to hospitals that have instituted a disaster protocol; and (3) for up to 72 hours from the time the hospital implements its disaster protocol. When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours have not elapsed since implementation of its disaster protocol.").

[17] *Id*.

[18] HHS, OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html (released Mar. 17, 2020); HHS, Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (last visited Mar. 24, 2020).

[19] For example, legislation pending on March 24, 2020 would require HHS to "issue guidance on the sharing of patients' protected health information pursuant to section 160.103 of title 45, Code of Federal Regulations (or any successor regulations) during the public health emergency declared by the Secretary of Health and Human Services under section 319 of the Public Health Service Act (42 U.S.C. 247d) with respect to COVID-19." H.R. 748, 116th Cong. § 3224 (2020).

[20] Cal. Civ. Code § 56.21(a).