Coppersmith Briefs

OCR Waives HIPAA BAA Requirements to Participate in Public Health and Health Oversight Activities

Erin Dunlap and Mel Soliz, Coppersmith Brockelman PLC

April 2, 2020

Today, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) makes it easier for HIPAA business associates to assist in COVID-19 efforts. Effective immediately, OCR is waiving the HIPAA business associate agreement requirements that might otherwise stand in the way of business associates participating in public health and health oversight activities during the COVID-19 nationwide public health emergency. *See* Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19 (Notice).

Under the HIPAA Privacy Rule (45 C.F.R. 164, Subpart E), if an organization provides services to a HIPAA covered health care provider or a health plan, and the organization has access to protected health information (PHI), it is a HIPAA business associate (BA) to that provider or plan and may only use or disclose that information as explicitly permitted in its business associate agreement (BAA) with that provider or plan, or as required by law. However, during this COVID-19 national emergency, public health and health oversight agencies (federal and state) have requested patient information from BAs and/or asked BAs to perform data analytics for the purposes of ensuring the health and safety of the public. Some BAs have been unable to participate because their BAAs do not expressly allow them to do so.

In today's Notice, OCR relaxes the BAA requirements during this nationwide public health emergency, stating that it will **not** impose penalties against a BA (or the provider or plan) if the BA uses or discloses PHI in good faith for permitted public health and health oversight activities, even if the BAA does not explicitly permit such use and disclosure.

- For permitted ***public health activities***, see 45 C.F.R. § 164.512(b) (such as reporting to a public health authority).

- For permitted ***health oversight activities***, see 45 C.F.R. § 164.512(d) (such as reporting to government authorities that oversee the health care system).

The BA must also inform the provider or health plan within ten (10) calendar days after the use or disclosure occurs. OCR does not state how that notice must occur, so we think written or oral notice is likely permissible but suggest a BA should follow any notice requirements in its BAA.

OCR gave the following examples of good faith uses and disclosures covered by the Notice:

- A use or disclose for or to the Centers for Disease Control and Prevention (CDC), or a similar state public health authority, for purposes of preventing or controlling the spread of COVID-19, consistent with 45 C.F.R. § 164.512(b); and

- A use or disclose for or to the Centers for Medicare and Medicaid Services (CMS), or a similar state health oversight agency, for purposes of overseeing and providing assistance for the health care system as it relates to the COVID-19 response, consistent with 45 C.F.R. § 164.512(d).

OCR makes clear that no other requirements or prohibitions under the HIPAA Privacy Rule, HIPAA Security Rule (45 C.F.R. 164, Subpart C) or HIPAA Breach Notification Rule (45 C.F.R. 164, Subpart D) are waived under this Notice, and specifically, under the HIPAA Security Rule, if BAs send electronic patient information to a public health authority or health oversight agency, they must do so securely.

OCR also notes this Notice does not waive other federal or state laws that may apply – or impact any breach of contract claims (*e.g.*, any claim a provider or plan may have against a BA for the use and disclosure of its patient information in this way).

Arizona Specific Alert: Arizona Business Associates are Required to Provide Access under the Enhanced Surveillance Advisory (Executive Order: 2020-13) (Mar. 23, 2020)

On March 23, 2020, Governor Doug Ducey issued an Enhanced Surveillance Advisory for COVID-19 (Executive Order 2020-13) in accordance with A.R.S. § 36-782(B), which gives the Arizona Department of Health Services (ADHS) and any local health authority the right to "access confidential information, including medical records, whenever ***and by whomever held*** and whether or not patient identify [sic] is known." (emphasis added). This order carries the force of law and would require BAs to provide access to ADHS and local health authorities. As explained above, the HIPAA Privacy Rule expressly requires use of contract language in the BAA that gives BAs permission to use and disclose PHI "as required by law." 45 C.F.R. §

164.504(e)(2)(ii)(A). Thus, BAs in Arizona may provide access to ADHS and local health authorities in accordance with the Enhanced Surveillance Advisory without relying on the OCR waiver to do so.

Erin Dunlap is a top-notch expert on health care data privacy and security issues. She regularly advises clients across the country on HIPAA and 42 C.F.R. Part 2 compliance, and state privacy and breach notification laws. Erin has extensive experience leading clients through privacy and security-related investigations and has successfully resolved numerous investigations (federal and state) without penalty or payment. Erin is affiliated with Coppersmith Brockelman on designated matters, and licensed in Missouri and Illinois.

Melissa Soliz focuses on HIPAA and 42 C.F.R. Part 2 compliance, health information exchange and networks (including compliance with the new information blocking rule), compliance with opioid treatment laws and regulations, data breaches and OCR investigations, as well as clinical research compliance and contracting.