

CHANGES IN HIPAA PRIVACY RULES 2020 DURING COVID-19

MGMA State Affiliate webinar
Thursday, March 26, 2020

Coordinated by:



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

1

HIPAA Monetary Penalties

In April 2019, HHS adjusted monetary penalties it will impose on healthcare organizations, health plans and their business associates for violating HIPAA.

This action changes HIPAA monetary penalties to a tiered system. Previously, there was a total annual fine limit of \$1.5 million for all HIPAA violations, regardless of an organization's level of culpability.

HHS announced the new tiered structure will be based on an organization's culpability and sets different annual limits for fines based on four penalty tiers.

Healthcare organizations that have taken steps to comply with HIPAA requirements or work quickly to mitigate violations will now face a smaller maximum penalty than organizations found neglectful.

2



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

2

HIPAA Monetary Penalties

HHS has identified four tiers of HIPAA violations based on severity: if an entity was unaware of the violation; the violation was due to reasonable cause and not neglect; the violation was due to neglect but the entity fixed it and; if the violation was due to neglect and not corrected in a timely manner,

The new tier structure for monetary penalties is now:

- **Tier 1 (no knowledge of violation):** \$100 to \$50,000 per violation; capped at \$25,000 per year
- **Tier 2 (reasonable cause):** \$1,000 to \$50,000 per violation; capped at \$100,000 per year
- **Tier 3 (willful neglect, corrected):** \$10,000 to \$50,000 per violation: capped at \$250,000 per year
- **Tier 4 (willful neglect, not corrected):** \$50,000 per violation; capped at \$1.5 per year

3



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

3

HIPAA Privacy Rule and Disclosures in Emergency Situations

- The HIPAA Privacy Rule always allows patient information to be shared for the following purposes and under the following conditions.
- **Treatment.** Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient.
 - *Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501.*

4



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

4

HIPAA Privacy Rule and Disclosures in Emergency Situations

- **Public Health Activities.** The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Covered Entities are permitted to disclose needed protected health information without individual authorization:
 - *To a public health authority, such as the CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability.*
 - *At the direction of a public health authority, to a foreign government agency that is acting in collaboration with the public health authority. See 45 CFR 164.512(b)(1)(i).*
 - *To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations. See 45 CFR 164.512(b)(1)(iv).*

5



Southern **Health** Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

5

HIPAA Privacy Rule and Disclosures in Emergency Situations

- **Disclosures to Prevent or Lessen a Serious and Imminent Threat.** Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider’s standards of ethical conduct.
- **Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification.** In general, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient’s illness, may not be done without the patient’s written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient).
 - *Where a patient has not objected to or restricted the release of protected health information, a Covered Entity may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient’s condition in general terms (e.g., critical or stable, deceased, or treated and released).*
- **Minimum Necessary.** For most disclosures, Covered Entities must make reasonable efforts to limit the information disclosed to that which is the “minimum necessary” to accomplish the purpose.
 - *Covered Entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances. For example, a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have COVID-19 is the minimum necessary for the public health purpose.*

6



Southern **Health** Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

6

Limited Waiver of HIPAA Sanctions and Penalties

- Effective March 15, 2020, HHS issued a bulletin announcing that HHS Secretary Alex Azar has exercised his authority to waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the HIPAA Privacy Rule.
- When such a waiver is issued, 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.

7



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

7

Limited Waiver of HIPAA Sanctions and Penalties

- Covered hospitals that meet the described criteria will have sanctions and penalties waived for non-compliance with the following provisions of the HIPAA Privacy Rule:
 - *the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b);*
 - *the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a);*
 - *the requirement to distribute a notice of privacy practices. See 45 CFR 164.520;*
 - *the patient's right to request privacy restrictions. See 45 CFR 164.522(a);*
 - *the patient's right to request confidential communications. See 45 CFR 164.522(b).*
- Importantly, the waiver applies only to hospitals that have instituted a disaster protocol. The waiver applies up to 72 hours from the time the hospital implements its disaster protocol or when the HHS declaration terminates – whichever is earlier. A hospital must then comply with the HIPAA Privacy Rule in its entirety.

8



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

8

Limited Waiver of HIPAA Noncompliance-Telemedicine

- On March 18, 2020, HHS's Office for Civil Rights (OCR) announced that it will not be imposing penalties for providers who use communication devices or other technologies that do not meet HIPAA's requirements in order to treat patients via telehealth.
- OCR is now permitting covered health care providers to use any remote communication devices or platforms to provide good-faith telehealth services.
 - *These telehealth services can be for any type of health care service, whether related to COVID-19 or not.*
- The only limitation on the type of communication technology is that it must be "non-public facing," meaning that it cannot share the patient's information publicly.
 - *For example, a covered health care provider could not publicly respond to a patient on Twitter or TikTok.*
 - *However, providers can use the private messaging functions of social media channels, like Facebook Messenger's video chat, or other commonly used applications for private video communication, like FaceTime or Skype. These communication methods may not typically meet HIPAA's stringent privacy and security standards and would normally be prohibited.*
- OCR recommends that covered health care providers alert patients of the privacy and security risks and take precautions where possible, such as enabling privacy mode, if innovative telemedicine platforms are utilized.

9



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

9

Limited Waiver of HIPAA Noncompliance-Telemedicine

- If covered health care providers want to use more secure platforms for patient communications during this time (though OCR says that they don't have to), OCR provided the following list of vendors that claim to sign BAAs with providers and be HIPAA-compliant (OCR hasn't independently verified this information though):
 - *Skype for Business*
 - *Updox*
 - *Vsee*
 - *Zoom for Healthcare*
 - *Doxy.me*
 - *Google G Suite Hangouts Meet*
- Covered entities should still consider privacy and security risks on both on the provider's and the patient's ends when making the switch to telehealth.
- These actions by the federal government do not change state laws.
 - *States must take specific action to loosen or waive their own requirements.*

10



Southern *Health* Lawyers, LLC
A SANDERS & MUSTARI LAW FIRM
ATLANTA / JACKSONVILLE / BIRMINGHAM

10

Limited Waiver of HIPAA Noncompliance-Telemedicine

- On March 20, 2020, OCR released a list of frequently asked questions to common concerns raised about its recent move to lift certain HIPAA penalties around telehealth use during the COVID-19 pandemic:
 - <https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf>

11



11

Questions?

Richard Sanders, Esq.
Southern Health Lawyers, LLC
rsanders@southernhealthlawyers.com
(404) 806-5575



12



12