HIPAA Hot Topics
HCCA Regional Conference Webinar

May 1, 2020

Allen Killworth
Bricker & Eckler

Bricker & Eckler ATTORNEYS AT LAW

0

Outline

Bricker & Eckler ATTORNEYS AT LAW

- COVID-19
  - Limited Waivers
  - Enforcement Discretion
- Access Issues
  - Right of Access Initiative
  - *Ciox* Decision
- New and Anticipated Regulations
  - NPP Rule Change – Part 2 inclusion
  - 2018 RFI
  - Penalty Reduction
- Recent Enforcement Actions

1

1

COVID-19

Bricker & Eckler ATTORNEYS AT LAW

On March 13, 2020, Secretary Azar issued a declaration of waiver under 1135 authority with various components, including:

> 2. Pursuant to Section 1135(b)(7) of the Act, I hereby waive sanctions and penalties arising from noncompliance with the following provisions of the HIPAA privacy regulations: (a) the requirements to obtain a patient's agreement to speak with family members or friends or to honor a patient's request to opt out of the facility directory (as set forth in 45 C.F.R. §164.510); (b) the requirement to distribute a notice of privacy practices (as set forth in 45 C.F.R. § 164.520); and (c) the patient's right to request privacy restrictions or confidential communications (as set forth in 45 C.F.R. § 164.522); but in each case, only with respect to hospitals in the designated geographic area that have hospital disaster protocols in operation during the time the waiver is in effect.

2

2

COVID-19

Bricker & Eckler ATTORNEYS AT LAW

These are <u>limited</u> waivers. Waived are:

(a) the requirements to obtain a patient's agreement to speak with family members or friends or to honor a patient's request to opt out of the facility directory (as set forth in 45 C.F.R. §164.510);

(b) the requirement to distribute a notice of privacy practices (as set forth in 45 C.F.R. § 164.520); and

(c) the patient's right to request privacy restrictions or confidential communications (as set forth in 45 C.F.R. § 164.522); but in each case, only with respect to hospitals in the designated geographic area that have hospital disaster protocols in operation during the time the waiver is in effect.

3

3

COVID-19

Only applicable after hospital implements disaster protocol for period of 72 hours. From Azar declaration:

> These waivers and modifications will become effective at 6:00 P.M. Eastern Standard Time on March 15, 2020, but will have retroactive effect to March 1, 2020, nationwide, and continue through the period described in Section 1135(e). Notwithstanding the foregoing, the waivers described in paragraph 2 above are in effect for a period of time not to exceed 72 hours from implementation of a hospital disaster protocol but not beyond the period described in Section 1135(e). The waivers described in paragraphs 1(c) and 2 above are not effective with respect to any action taken thereunder that discriminates among individuals on the basis of their source of payment or their ability to pay.

4

4

COVID-19

Enforcement discretion

1. Telehealth services – issued 3/17/20.
   - Notice that OCR would waive any potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency.
   - Applies to good faith use of any non-public facing remote communication product that is available to communicate with patients for any telehealth treatment or diagnostic purpose. Technology that may be used includes popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video or Skype. Use of public facing applications, such as Facebook Live, are *not* permitted.
   - Includes use of telehealth for *any* patient. Services do *not* have to be directly related to COVID-19.
   - Providers encouraged to use technology with vendors willing to enter into business associate agreements. However, penalties will not be imposed for lack of business associate agreement.
   - Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

5

5

COVID-19

Enforcement discretion

2. Public health disclosures by Business Associates – issued 4/2/20.
   - OCR will not impose penalties against a BA or CE when BA makes disclosure to public health authorities or health oversight agencies during the public health emergency if:
     - BA makes good faith use or disclosure for public health activities consistent with 45 CFR 164.512(b) or health oversight activities consistent with 45 CFR 164.512(d)
     - BA informs the CE within ten calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).
3. Community-based testing sites – issued 4/9/20.
   - OCR will not impose penalties for violations in connection with a CE's or BA's good faith participation in the operation of a COVID-19 Community-Based Testing Site.

6

6

Access Issues – Right of Access Initiative

- November 2019 HHS announced the Right of Access Initiative, a plan to vigorously enforce patient access rights. OCR Director Roger Severino: "We aim to hold the health care industry accountable for ignoring peoples' rights to access their medical records and those of their kids."
- Two cases with formal resolutions announced:
  - Bayfront Health. Resolved complaint regarding single case of failing to provide mother with records of her child. Only after OCR intervened were records disclosed more than nine months after request. $85,000 penalty and corrective action plan.
  - Korunda Medical. Resolved complaints alleging that Korunda failed to forward a patient's medical records in electronic format to a third party, failed to provide them in the requested electronic format, and charged more than allowed by HIPAA. $85,000 penalty and corrective action plan. Director Severino: "For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia. We hope our shift to the imposition of corrective actions and settlements under our Right of Access Initiative will finally wake up healthcare providers to their obligations under the law."

7

7

Access Issues – *Ciox* Decision

- In *Ciox Health vs. Azar, et al.*, No. 18-CV-0040 (D.D.C. January 23, 2020), a federal court vacated the "third-party directive".
- 45 CFR 164.524 limits charges to a "reasonable, cost-based fee" when an "individual requests a copy" of his/her PHI.
- 2016 guidance from HHS attempted to change this fee limitation to apply to requests to send PHI to a third party.

  https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- Result of decision: The fee limitation set forth at 45 CFR 164.524(c)(4) will apply only to an individual's request for access to their own records, and does not apply to an individual's request to transmit records to a third party.

8

New and Anticipated Regulations

Changes to NPP Rule

- CARES Act
- Requires HHS to update 45 CFR 164.520 within one year, so that CEs provide notice of privacy practices regarding Part 2 patient records including: (1) a statement of the patient's rights, including self-pay patients, with respect to PHI and a brief description of how the individual may exercise these rights and (2) a description of each purpose for which the CE is permitted or required to use or disclose PHI without the patient's written authorization.

.

9

New and Anticipated Regulations

RFI – December 2018

- HHS reviewing comments received. Anticipated that rulemaking to follow. Timeframe unannounced. HHS had requested comments regarding changes related to:
  - Promoting information sharing for treatment and care coordination and/or case management by amending the Privacy Rule to encourage, incentivize, or require CEs to disclose PHI to other CEs.
  - Encouraging CEs to share treatment information with parents, loved ones, and caregivers of adults facing health emergencies, with a particular focus on the opioid crisis.
  - Implementing the HITECH Act requirement to include, in an accounting of disclosures, disclosures for treatment, payment, and health care operations from an EHR in a manner that provides helpful information to individuals, while minimizing regulatory burdens and disincentives to the adoption and use of interoperable EHRs.
  - Eliminating or modifying the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of providers' Notice of Privacy Practices.

10

.

10

New and Anticipated Regulations

Promoting information sharing --

- Questions regarding access rights and length of time to respond.
  - "How feasible is it for CEs to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules?"
  - "Should CEs be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access?"
- Questions regarding requiring disclosure for treatment.
  - "Do health care providers currently face barriers or delays when attempting to obtain PHI from CEs for treatment purposes?"
  - "Should CEs be required to disclose PHI when requested by another CE entity for treatment purposes? Should the requirement extend to disclosures made for payment and/or health care operations purposes…?"
  - "Should OCR create exceptions or limitations to a requirement for CEs to disclose PHI to other health care providers (or other CEs) upon request?"
- Questions regarding other barriers.
  - "What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent [with the Information Blocking rules]?"
  - "Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard?"

11

11

New and Anticipated Regulations

Bricker & Eckler ATTORNEYS AT LAW

Sharing for mental health / opioid reasons --

- "What changes can be made to the Privacy Rule to help address the opioid epidemic? What risks are associated with these changes?"
- "Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment information of their minor children, especially where the child has substance use disorder (including opioid use disorder) or mental health issues, or are existing permissions adequate?"
- "Should any changes be made to specifically allow parents or spouses greater access to the treatment information of their children or spouses who have reached the age of majority?"
- "Should changes be made to allow adult children to access the treatment records of their parents in certain circumstances, even where an adult child is not the parent's personal representative?"

12

12

New and Anticipated Regulations

Bricker & Eckler ATTORNEYS AT LAW

Accounting of disclosures --

- "Is the system able to distinguish between "uses" and "disclosures" as those terms are defined under the Privacy Rule at 45 CFR 160.103?"
- "To what extent do CEs maintain a single, centralized EHR system versus a decentralized system (*e.g.,* different departments maintain different EHR systems, and an accounting of disclosures for TPO would need to be tracked for each system)?"
- "If an EHR is not currently able to account for disclosures of an EHR to carry out TPO, what would be the burden, in time and financial costs, for CEs and/or their vendors to implement such a feature?"
- "If CEs are unable to modify existing systems or processes to generate a full accounting of disclosures for TPO (*e.g.,* because modification would be prohibitively costly), should OCR instead require CEs to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual's request for an accounting of disclosures for TPO?"
- "The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed through, an EHR? Why or why not?"

13

13

New and Anticipated Regulations

Bricker & Eckler ATTORNEYS AT LAW

Notice of privacy practices --

- "What is the burden, in economic terms, for covered health care providers that have a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's NPP?"
- "For what percentage of individuals with whom a direct treatment provider has a relationship is such a covered health care provider unable to obtain an individual's written acknowledgment? What are the barriers to obtaining it?"
- "What benefits or adverse consequences may result if OCR removes the requirement for a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgment of the receipt of the provider's NPP?"
- "Are there modifications to the content and provision of NPP requirements that would lessen the burden of compliance for covered entities while preserving transparency about covered entities' privacy practices and individuals' awareness of privacy rights?"

14

14

New and Anticipated Regulations

Bricker & Eckler ATTORNEYS AT LAW

Penalties reduced!

- In 2019, three of four tiers of HIPAA penalties were reduced through notice of enforcement discretion.
- HITECH Act increased penalties with maximum penalty of $1.5M per year. Previously this was applied to all four tiers.
- New interpretation of this language results in OCR applying lower maximum annual penalties to three tiers of penalties.
- Regulations codifying these changes is expected in near future.

15

15

New and Anticipated Regulations

Penalties reduced!

	Penalty range for each violation	Previous annual max	New annual max
Tier 1: Did not know	$100-$50,000	$1,500,000	$25,000
Tier 2: Reasonable cause	$1,000-$50,000	$1,500,000	$100,000
Tier 3: Willful neglect - corrected	$10,000-$50,000	$1,500,000	$250,000
Tier 4: Willful neglect - not corrected	$50,000	$1,500,000	$1,500,000

16

16

Recent Enforcement Actions – Failure to Conduct/Act on Risk Analysis

- Steven Porter, MD (March 2020)
  - $100,000 settlement. HHS investigated after breach report filed related to a BA dispute.
  - Investigation determined practice had never conducted a risk analysis.
  - CAP required practice to: (1) conduct a risk analysis and formulate a risk analysis plan, subject to the approval of HHS; (2) develop and implement a risk management plan, subject to the approval of HHS; (3) adopt/revise HIPAA policies, subject to the approval of HHS; (4) review and revise its HIPAA training materials, subject to the approval of HHS; (5) report non-compliance to HHS.
- University of Rochester Medical Center (November 2019)
  - $3M settlement for failure to encrypt mobile devices resulting in theft of PHI.
  - 2013 breach reported to HHS of lost unencrypted flash drive containing PHI (unclear how resolved with HHS). In 2017, URMC reported breach due to theft of unencrypted laptop (personal laptop of resident) containing PHI of 43 individuals.
  - OCR found (1) URMC failed to conduct risk analysis including risks of unencrypted mobile devices, (2) URMC failed to implement policies to reduce risks, for removal of hardware with ePHI and to encrypt ePHI.
  - CAP requires URMC to conduct/adopt (1) risk analysis, (2) risk management plan, (3) process for evaluating environmental or operational changes that affect security of ePHI, (4) updated HIPAA policies and procedures, all of which require HHS approval. Also requires report of potential non-compliance to HHS and annual report to HHS.

17

17

Recent Enforcement Actions – Improper Disclosure / Breach Issues

- Sentara Hospitals (November 2019)
  - $2.175M penalty settlement for failure to notify HHS of breach. Mailed PHI of 577 patients to wrong addresses. Information included name, account numbers, and dates of services. Sentara reported breach affecting 8 individuals "because Sentara concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information, or other medical information, no reportable breach of PHI had occurred."
  - Sentara "allowed their parent corporation and business associate, Sentara Healthcare, to [use] PHI on their behalf and to provide services involving the disclosure of PHI without [a BAA]."
  - CAP required updated policies, training, reporting.
- Texas Health & Human Services Commission (November 2019)
  - $1.6M determination. Texas state agency administering long term health services reported breach affecting 6,617 individuals when internal software application was inadvertently moved from private to public server.
  - Investigation determined failure of internal audit controls meant agency was unable to determine how many unauthorized persons accessed the PHI.
  - CAP required practice to: (1) conduct a risk analysis and formulate a risk analysis plan, subject to the approval of HHS; (2) develop and implement a risk management plan, subject to the approval of HHS; (3) adopt/revise HIPAA policies, subject to the approval of HHS; (4) review and revise its HIPAA training materials, subject to the approval of HHS; (5) report non-compliance to HHS.

Recent Enforcement Actions – Miscellaneous

- Elite Dental Associates (October 2019)
  - EDA paid $10,000 settlement for improper disclosure of PHI on social media.
  - EDA responded to a patient's post on social media criticizing the practice. EDA's response including patient's name and details of patient's condition. HHS investigation revealed multiple responses by EDA with this problem.
  - CAP included 2 years of HIPAA compliance monitoring by OCR. Requires EDA to adopt HIPAA policies and have approved by HHS, report any potential non-compliance to HHS, and annual reports to HHS. HHS noted: "OCR accepted a substantially reduced settlement in consideration of [EDA's] size, financial circumstances, and cooperation…".
- Touchstone Medical Imaging (May 2019)
  - $3M settlement. Touchstone was notified by the FBI that one of its servers allowed public access to patient information. Touchstone initially claimed no PHI was exposed.
  - OCR investigation resulted in Touchstone admitting PHI of 300,000 individual was exposed. OCR found Touchstone did not thoroughly investigate until months after notice from FBI, resulting in eventual breach notices being untimely.
  - OCR Director Severino: "Covered entities must respond to suspected and known security incidents with the seriousness they are due…"

Conclusion

Allen Killworth

614-227-2334

akillworth@bricker.com

20