



Update on HIPAA and CURES Act Regulations - 2021

Jeremy W. Meisinger
Samuel R. Hoff

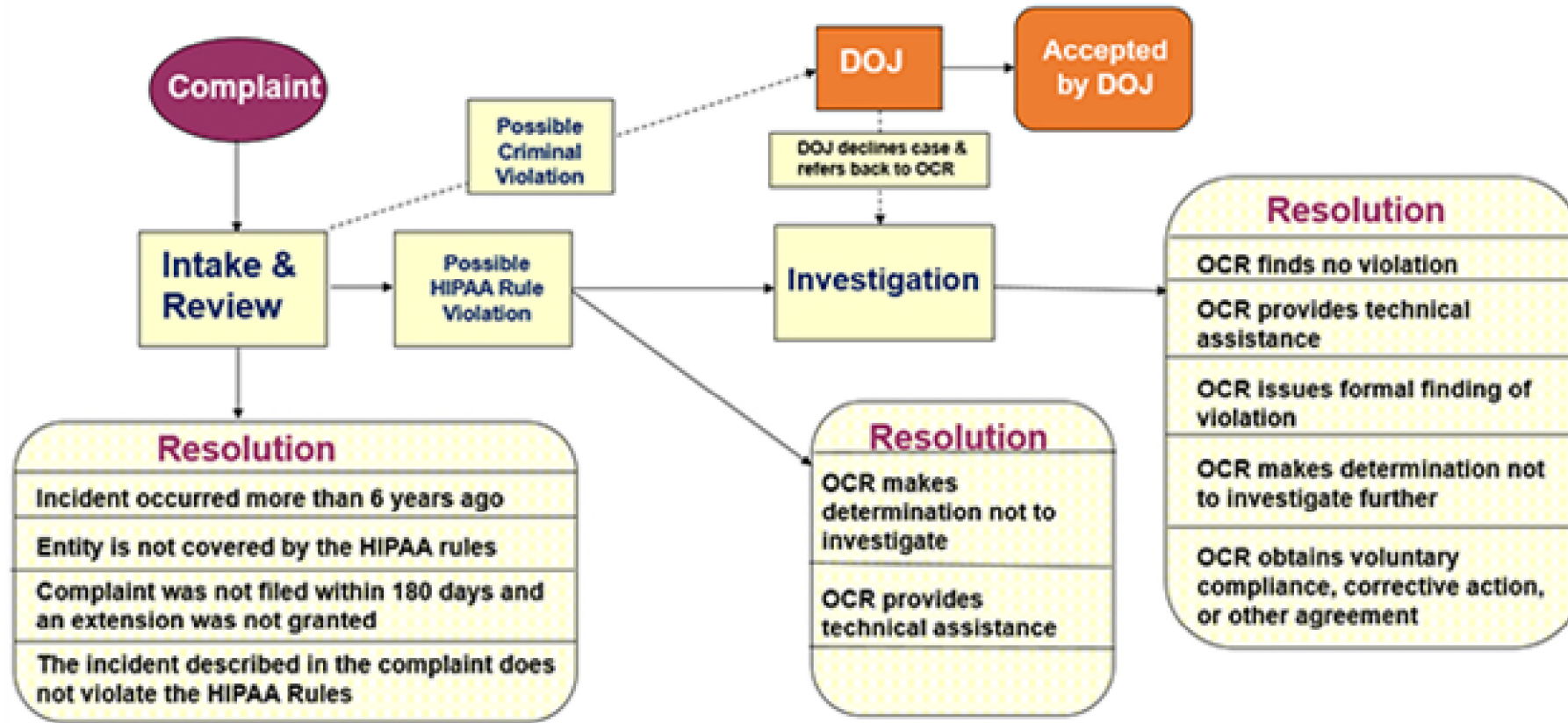


September 29, 2021

- Enforcement and Penalties
- HIPAA and COVID-19
- Recent Settlements
- OCR Leadership and Enforcement Priorities Going Forward
- Upcoming Regulatory Changes to HIPAA
- Current Regulatory Status of CURES Act Rules

- The U.S. Department of Health and Human Services (“HHS”) Office for Civil Rights (“OCR”) is responsible for enforcing HIPAA’s Privacy, Security, and Breach Notification Rules.
- OCR has several ways of enforcing HIPAA:
 - Investigating complaints;
 - Conducting compliance reviews to determine whether covered entities are in compliance; and
 - Performing education and outreach to foster compliance.
- Complaints are, by far, the primary way in which OCR learns about potential HIPAA violations.
 - Since the Privacy Rule went into effect in April 2003, OCR has received, on average, 14,000 complaints per year.
 - Complaints are typically filed by patients and current or former employees.

HIPAA Complaint Process



- OCR works in conjunction with the Department of Justice (“DOJ”) to refer possible criminal violations of HIPAA.
- OCR reports, however, that it only refers approximately 1% of the total complaints that it receives to the DOJ for investigation.
- In the past calendar year, the DOJ has only reported one case in which an individual or entity received criminal punishment for improper use or disclosure of Protected Health Information (“PHI”), and the individual in question was not even a covered entity.
 - In July 2021, a Texas woman pled guilty to “conspiracy to obtain information from a protected computer.” She allegedly broke into a health care provider’s electronic health record (“EHR”) system, stole PHI, and repackaged the PHI in the form of fraudulent physician orders which she sold to medical equipment manufacturers. She received 30 months in federal prison.

- Civil penalties are much more common. They typically fall into one of four tiers:
 - **Tier 1**. Covered entity was unaware of the violation and could not have reasonably avoided it. Minimum fine of \$100/violation up to \$50,000.
 - **Tier 2**. Covered entity should have been aware of the violation but could not have avoided it even with a reasonable amount of care. Minimum fine of \$1,000/per violation up to \$50,000.
 - **Tier 3**. Covered entity willfully neglected HIPAA rules, but made an attempt to correct the violation. Minimum fine of \$10,000/per violation up to \$50,000.
 - **Tier 4**. Covered entity willfully neglected HIPAA rules, and made no attempt to correct the violation. Minimum fine of \$50,000/per violation (and no cap).
- OCR claims that it likes to resolve HIPAA violations using non-punitive measures such as voluntary compliance or the issuance of technical guidance.
- OCR will implement monetary penalties where violations are serious, have been allowed to persist for a long time, or there are multiple areas of noncompliance.

- In response to the COVID-19 nationwide public health emergency, OCR has issued several HIPAA bulletins and “Notifications of Enforcement Discretion Guidance” that apply to HIPAA enforcement under the circumstances of the pandemic.
- OCR has announced that it will not impose penalties for noncompliance where a covered entity shows “good faith” in:
 - Using online or web-based scheduling applications for the scheduling of vaccination appointments;
 - Participating in the operation of a community-based testing site; or
 - Providing telehealth using video-based communication technology.
- OCR has also issued guidance regarding the regulatory permissions that covered entities may rely on to disclose PHI to first responders so that they may take extra precautions or use personal protective equipment, where necessary.

- Aside from the flexibility and leniency that OCR is affording covered entities in connection with COVID-19, the settlements listed on the OCR website over the past three years show a mix of “classic” enforcement and new trends.
- “Classic” enforcement examples include:
 - Failure to terminate an ex-employee’s access to PHI.
 - In October 2020, the City of New Haven, Connecticut, agreed to pay \$202,400 to settle allegations that it failed to properly disable the credentials of an employee upon termination. The former employer later returned to her old office at a City-run public health clinic and used her still-active credentials to download 498 patients’ PHI onto a USB drive.
 - Failure to provide notice of a PHI breach.
 - In November 2019, a hospital network in Virginia and North Carolina agreed to pay \$2.175 million to settle allegations that it mailed 577 patients’ PHI to wrong addresses. It reported this breach as affecting only eight patients because it incorrectly concluded that the remaining 569 patients’ mailings did not include patient diagnosis, treatment, or medical information.
 - Violations related to business associates.
 - In December 2018, a Florida physician group agreed to pay \$500,000 to settle allegations that it contracted with a billing company without a BAA and did not have a policy requiring BAAs. The billing company EHR system was faulty and 8,885 patients’ names, DOBs, and SSNs subsequently became viewable online.

- Beyond the regular, “classic” enforcement that has occurred over the past three years, we see three new enforcement trends:
 - **Right of Access**. Covered entities improperly refusing to grant patients access to their PHI.
 - **Cyberattacks / Unprotected EHR**. In today’s world, PHI stored electronically is typically much more vulnerable to predators than hard copies of PHI stored in an office cabinet.
 - **Media-Related Disclosures**. Covered entities improperly disclose PHI on smart phone apps, through social media, or to traditional media outlets.

- This is the major enforcement trend in HIPAA enforcement today.
- In the past calendar year, OCR has reported 17 settlements with covered entities. 13 of these settlements were related to the Right of Access Initiative.
- The Right of Access Initiative stems from the Privacy Rule, which requires “that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient’s request.”
- Historically, OCR did not devote much attention to “right of access” enforcement.
- In early 2019, in response to a rising number of complaints, OCR announced the Right of Access Initiative, which promised to vigorously enforce the rights of patients to receive copies of their medical records promptly and without being overcharged.

■ Recent settlements:

- In September 2021, a pediatric hospital in Nebraska agreed to pay \$80,000 to settle allegations that it failed to provide a parent with timely access to her minor daughter's medical records. The hospital provided some records, but did not provide all of the requested records despite the parent's multiple follow-up requests.
- In March 2021, a hospital in Massachusetts agreed to pay \$65,000 to settle allegations that it did not provide a patient with timely access to her records. The patient had previously filed a complaint which led to OCR providing the hospital with technical assistance. OCR later learned that the hospital still had not responded to the same patient's record request, though, which led to the monetary settlement.
- In January 2021, a health system in Arizona agreed to pay \$200,000 to settle allegations that it did not provide patients with timely access to their records. In particular, OCR cited two instances in which a patient submitted a record request and did not receive the records for 5-6 months.

- Based on the dollar amounts of the Right of Access Initiative settlements, it seems that OCR does not consider the harm caused by a right-of-access violation to be as great as the harm caused by an improper disclosure.
- OCR is staying true to its initiative, though:
 - In June 2021, a diabetes treatment provider in West Virginia agreed to pay \$5,000 to settle such an enforcement action.
 - OCR is apparently comfortable utilizing its resources to achieve minor settlements in the interest of incentivizing covered entities to provide patient access as required by the Privacy Rule.
- Recommendations for covered entities:
 - Ensure that patient/HIPAA intake forms, e.g., Authorization for Use and Disclosure of PHI, have been reviewed by counsel and are in use.
 - Enact written policies and procedures to ensure that patient record requests are handled in a timely manner, staff understand how to handle a request by a parent, etc.

■ Recent settlements:

- In January 2021, a health insurer in New York agreed to pay \$5.1 million to settle allegations stemming from a breach that affected over 9.3 million people. The breach occurred in September 2015, when cyber-attackers gained access to the insurer's system, installed malware, and conducted reconnaissance activities that led to the impermissible disclosure of PHI.
- In July 2020, a non-profit health system in Rhode Island agreed to pay \$1.04 million to settle allegations stemming from the theft of an unencrypted laptop. The laptop in question contained EHR for 20,431 patients. The system failed to encrypt laptops that it issued to employees even after it had previously determined that it was reasonable and appropriate to do so.
- In October 2018, one of the nation's largest health benefit companies agreed to pay \$16 million to settle allegations stemming from the largest U.S. health data breach in history, which exposed the EHR of 79 million patients. Cyber-attackers gained access to the company's system through phishing emails sent to a subsidiary's employees. It only took one employee to respond to a phishing email for the cyber-attackers to gain access. The cyber-attackers then launched a "continued and targeted" attack on EHR for two months before they were detected.

- Recommendations for covered entities:
 - Confer with external IT consultant regarding your system's level of vulnerability. *This may be advisable even if you have internal IT personnel, i.e., it is helpful to have a second set of professional eyes scan for issues from time to time.*
 - Ensure that policies and procedures related to data protection and employee and contractor handling of company property containing EHR, e.g., laptops and mobile devices, have been reviewed by counsel and are in use.
 - Provide employees with training regarding phishing emails and other cyberattack schemes, and breach reporting.

- Recent settlements:
 - In October 2019, a health system in Florida agreed to pay \$2.15 million to settle multiple allegations, including that it impermissibly allowed a reporter access to an operating room, which enabled the reporter to take a photo of PHI and share the photo on social media.
 - In October 2019, a dental practice in Texas agreed to pay \$10,000 to settle allegations that it posted a patient's last name and details of the patient's health condition online in response to a negative Yelp review that the patient posted.
 - In November 2018, an allergy treatment provider in Connecticut agreed to pay \$125,000 to settle allegations that it improperly disclosed a patient's PHI to a local TV reporter. The patient initially contacted the TV station to report a dispute between her and the provider. The provider then impermissibly disclosed the patient's PHI to the reporter in an attempt to explain the story.
 - In September 2018, two hospitals in Massachusetts collectively agreed to pay \$999,000 to settle allegations that they improperly disclosed patients' PHI when they invited film crews onto their respective premises to film an ABC television documentary series without obtaining patients' consent.

- Recommendations for covered entities:
 - HIPAA permits disclosures of PHI for “health care operations,” which may include conducting or arranging for legal services, *but defending oneself in the court of public opinion is not the same as defending oneself in a court of law.*
 - Never disclose PHI to a third-party unless you have conferred with counsel.
 - Small practices and social media managers of large providers: *Never post on social media while angry! Stop and take a breath!*
 - Large providers should ideally assign a single individual to handle communications with the media, public statements, and/or social media, and expressly prohibit other employees from engaging in same.
 - Ensure that media-related policies and procedures have been reviewed by counsel and are in use.

Enforcement Priorities Going Forward

- The recent settlements discussed span the final two years of the Trump administration and the first year of the Biden administration.
- Whether these enforcement trends continue depends, to an extent, on OCR's leadership going forward.
- Robinsue Frohboese, the Acting Director of OCR, has been with the agency since 2000. She has served as the Acting Director during four Administrative transitions.
- She was integral to the initial implementation of the Privacy Rule and is a strong proponent of the current Right of Access Initiative.

In August 2021, she was quoted as saying, *"It should not take a federal investigation before a HIPAA covered entity provides a parent with access to their child's medical records" and that "covered entities owe it to their patients to provide timely access to medical records."*



Enforcement Priorities Going Forward

- It is thus a safe bet that OCR will continue to push the Right of Access Initiative in the near future (at least so long as Acting Director Frohboese leads the agency).
- We can also prognosticate OCR enforcement under Biden by considering same under Obama, who oversaw the passage of the HITECH Act and Omnibus Rule (which required BAAs and provided for directly liability of business associates for HIPAA violations).
- Obama's focus on protecting PHI in the modern age may suggest that Biden's OCR will continue its focus on cyberattacks and media-related disclosures (as it should).
- Business associate violations may also be the subject of renewed OCR focus.

■ Timeline of HIPAA Rulemaking

- December 2018 – Request for Information related to potential upcoming changes to HIPAA.
- December 10, 2020 – OCR releases a Notice of Proposed Rulemaking.
- January 21, 2021 – OCR publishes the Proposed Rule in the Federal Register and seeks public comment.
- March 22, 2021 – OCR extends the comment period for the Proposed Rule from to May 6, 2021.
- May 6, 2021 – OCR receives cumulatively about 1,400 comments on the Proposed Rule.

- Major Provisions of the Proposed Rule
 - Changes to requirements related to Notices of Privacy Practices.
 - Changes related to coordination of care.
 - Changes to disclosures related to emergencies.
 - Expansion of individual right of access.

- Notice of Privacy Practices
 - Eliminating requirement to obtain an individual's written acknowledgement of receipt of a direct treatment provider's notice of privacy practices.
 - Modifying the content requirements of notices with respect to PHI and exercising rights to access PHI.

- **Coordination of Care**
 - Creating an exception to the “minimum necessary” standard for individual-level care coordination and case management, permitting disclosures between health plans and health care providers for care coordination and case management functions.
 - Clarifying the scope of covered entities’ ability to disclose PHI to social services agencies, community-based organizations, home and community-based service providers, and similar third parties, to facilitate care coordination.

■ Emergency Disclosures

- Replacing the “professional judgment” standard for emergency disclosures to a “good faith-based” standard, permitting additional disclosures in emergencies.
- Expanding the ability of covered entities to disclose PHI in situations in which a threat is “serious and reasonably foreseeable,” as opposed to “serious and imminent.”

■ Individual Right of Access

- Strengthens right to inspect PHI in person, including inspecting and taking pictures of PHI.
- Shortening covered entities' required response time to 15 calendar days (from 30) with a possibility of a 15 day extension (from 30).
- Reducing identity verification requirements for individuals.
- Creating mechanism for individuals to direct sharing of PHI in an EHR among covered health providers by requiring covered entities to submit an individual's request to another covered entity and receive records in an EHR.
- Requiring electronic PHI to be provided at no cost in certain circumstances.
- Amending the fee structure for responding to requests to direct records to a third party.

- **Comments on the Proposed Rule**
 - How will the new HIPAA regulations be finalized with the Interoperability Rules?
 - How will coordinated care requirements interact with stricter state laws?
 - Will non-covered entities that will receive PHI under the proposed rule adequately protect that PHI?

- Finalizing Rulemaking
 - OCR received over 1400 comments on the Proposed Rule.
 - The effective date of a final rule would be 60 days after publication.
 - OCR has stated that it anticipates the compliance date would be 180 days following the effective date.

■ Information Blocking Rule

- Came into effect on April 5, 2021, following an adjustment in the applicability date from November 2, 2020.
- Prior to October 6, 2022, the information blocking rule applies only to the data elements represented in the United States Core Data for Interoperability (USCDI) standard.
- ONC guidance states with respect to enforcement that “[f]or health care providers, HHS must engage in future rulemaking to establish appropriate disincentives as directed by the 21st Century Cures Act.”

■ Civil Monetary Penalty Rule

- The HHS Office of the Inspector General is currently engaged in rulemaking to establish enforcement dates.

- The Information Blocking Rule and Providers
 - HHS guidance on the Information Blocking Rule has been frustratingly vague as applied to providers, because most of the Rule preamble and most HHS guidance focuses on health IT issues.
 - HHS defines “information blocking” as an activity that “is likely to interfere with access, exchange, or use of electronic health information.”

- The Information Blocking Rule and Providers
 - HHS’ “examples” of information blocking are vague and do not address the practical questions of providers, because they are:
 - Abstract (“[i]mplementing health IT in ways that are likely to [...] [r]estrict the access, exchange, or use of EHI”); or
 - They specifically address to health IT implementation, and not interactions with patients.

- The Information Blocking Rule and Providers
 - The Information Blocking Rule applies to notes as defined by USCDI.
 - This category includes (1) consultation notes, (2) discharge summary notes, (3) history and physical imaging narratives, (4) laboratory report narratives, (5) pathology report narratives, (6) pathology report narratives, (7) procedure notes, and (8) progress notes.
 - “[N]one of the eight types of notes currently represented within the USCDI are limited based on the type or specialty of the professional who authors them.”

- The Information Blocking Rule and Providers
 - Non-final clinical information, including “draft clinical notes or incomplete test results that are pending confirmation” is not necessarily within the purview of the Information Blocking Rule.
 - HHS states that “[d]raft clinical notes and laboratory results pending confirmation are [...] examples of data points that may not be appropriate to disclose or exchange until they are finalized.”
 - HHS hinges the analysis on whether “such data are used to make health care decisions about an individual.”

■ The Information Blocking Rule and Providers

- HHS' guidance on delays in accommodating access requests arguably contradicts its statements discussed on the prior slide.
- HHS states that “[i]t would likely be considered interference for purposes of information blocking if a health care provider established an organizational policy that [...] imposed delays on the release of lab results for any period of time in order to personally inform the patient of the results before a patient can electronically access such results.”
- But HHS does not state whether they are referring to “draft” or “final” results.
- HHS also acknowledges that where state law requires a delay in communication, such delay is not information blocking.