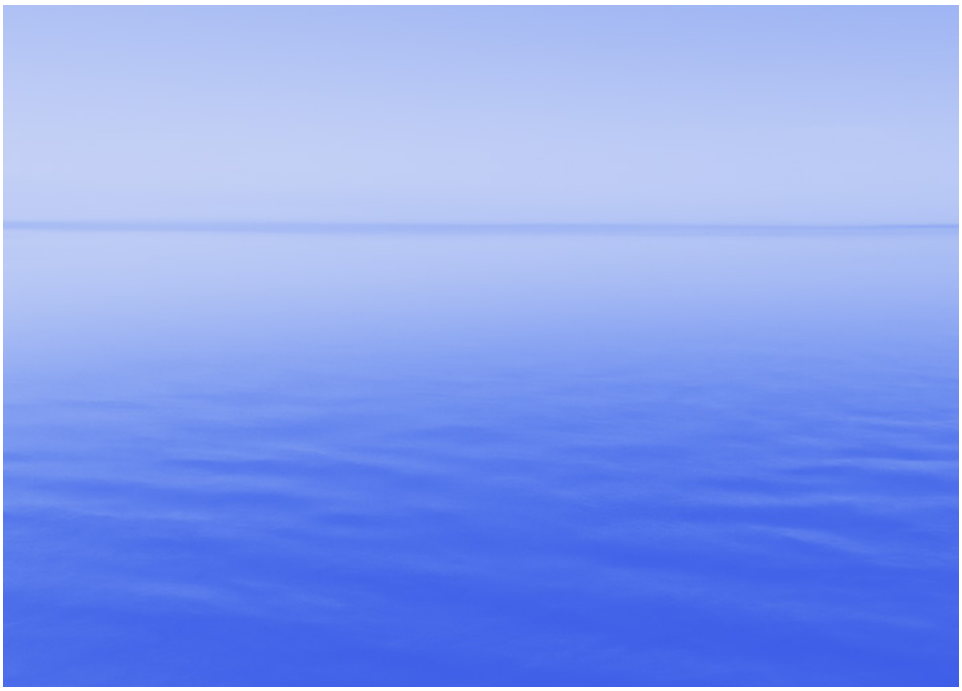
Clearwater

Whitepaper

More Breaches, More Settlements, More Investigations

A Pandemic View of OCR Enforcement of HIPAA Requirements

Table of Contents



© Clearwater | All Rights Reserved | 14.3

Introduction

Around the globe, most industries have experienced an increase of cyber breaches in the last few years, but none likely as hard-hit and specifically targeted in 2020 as healthcare.

As a result, we saw another big jump in the number of healthcare data breaches of 500 or more records reported to the Office for Civil Rights (OCR). The HIPAA Journal reports that there were a total of 616 such breaches in 2020, up more than 20% from the 2019 figure of 510.

Pandemic practices

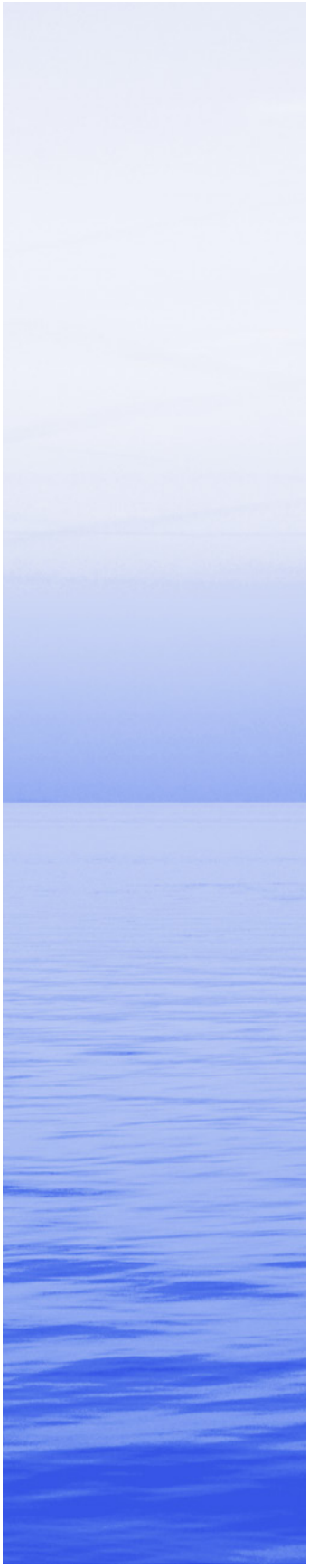
While we have seen strong evidence that the pandemic has led to an increase in healthcare-related data breaches and targeting, the pandemic didn't give organizations a free pass to ignore HIPAA requirements.

An initial bulletin issued by OCR on February 3 of last year emphasizing that HIPAA still applies during a pandemic was followed by a series of communications related to waivers and enforcement discretion:

- March 13, 2020: Enforcement discretion community-based testing sites
- March 15, 2020: Privacy rule waiver hospitals in disaster protocol
- March 17, 2020: Enforcement discretion on telehealth
- April 2, 2020: Enforcement discretion for business associates to aid federal and state health and oversight agencies

But what did any of that actually mean for healthcare organizations? Where were the differences relating to waivers and enforcement?

OCR can decide in any circumstances to exercise enforcement discretion, and in some instances like this, OCR may say if they may waive penalties. But don't rest on your laurels. You could still face penalties, for example, if your state's attorney general chooses to litigate. You could also have to deal with a variety of other issues and penalties related to other contractual and legal obligations. Plus, there are additional agencies that may come into play, like the Federal



© Clearwater | All Rights Reserved | 14.3

Trade Commission if you're using a SaaS for your video conferencing telehealth components, if you have breaches or other security issues.

But it's important to remember, even during a pandemic or other waiver periods, your HIPAA requirements do not change or go away so breach prevention must remain front-and-center.

What's considered a HIPAA breach?

As part of the HITECH Act, OCR must make public all breaches reported to the Secretary of Health and Human Services that affect 500 or more individuals. These are updated regularly and shared with the public in OCR's Breach Portal.

But what's considered a breach in relation to the Health Insurance Portability and Accountability Act and how does a breach end up in the portal?

According to 45 C.F.R. 164.402, HIPAA rules define a breach as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the [HIPAA Privacy Rule] that compromises PHI security or privacy.

HIPAA's Breach Notification Rule then requires all covered entities to make affected individuals, aware when of when PHI security and privacy has been breached, for example when it's been disclosed without consent or used without permission. This is applicable even if the covered entity isn't yet sure if the breach resulted in compromised PHI or the exact number of affected records. There is also a notification time period that's applicable–within 60 days of after breach discovery.

When breaches affect 500 or more people, the covered entity must also report the breach to the Department of Health and Human Services (HHS) OCR as well as a prominent media outlet that serves the area where the breach happened.

> Shortly after the World Health Organization (WHO) deemed COVID-19 a pandemic, threat actors turned up the heat, coming hard for healthcare organizations that, because of social distancing and stay-at-home mandates, picked up the pace adopting new technologies to facilitate telehealth and related practice modernizations.

© Clearwater | All Rights Reserved | 14.3

OCR investigations and penalties

Failing to safeguard PHI can result in a range of penalties[1] from fines to criminal and civil liabilities. These penalties are designed to deter—and hold accountable—covered entities from disregarding HIPAA requirements.

OCR can issue a range of tiered penaltiesi for a breach related to culpability, which increase based on severity. Tier 1 violations, for example, can be as little as $100, increasing to $1,000 for Tier 2, then $10,000 for Tier 3, and finally Tier 4 at $50,000.

Tier 1, No Knowledge: The covered entity had no knowledge or through diligence could not have known/avoided the breach.

Tier 2, Reasonable Cause: The covered entity should have known, but the beach could not be known/avoided with reasonable diligence.

Tier 3, Willful Neglect, Corrected: The covered entity displayed willful neglect of the HIPAA rules and made an attempt to correct the issue.

Tier 4, Willful Neglect, Not Corrected: The covered entity displayed willful neglect of HIPAA rules and did not try to correct the issue.

In addition to investigating PHI-related breaches, in 2019, OCR announced[2] its HIPAA Right of Access Initiative, indicating it would also make it a priority to support individuals' rights to access their health records in a timely manner and at reasonable cost as outlined by the HIPAA Privacy Rule.

By late December 2020, OCR announced its 13th settlement related to enforcement of its HIPAA Right of Access Initiative. There were 19 enforcement OCR actions overall for the year, establishing a new high mark for the regulatory body and nearly doubling the activity seen in each of the previous three years.

Ongoing investigations

As a result of the HIPAA complaints and Right of Access, OCR, at any given time, will have hundreds of cases to investigate. Many of those cases are actively tracking for settlement, and in general, it can take years to complete an OCR investigation. So

1 https://www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties

2 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ucmc/index.html

© Clearwater | All Rights Reserved | 14.3

what we're seeing with case settlement actions in 2020 is likely the result of those investigations coming to an end, as well as the Right of Access Initiative push.

Here's a quick look at some of the recent HIPAA enforcement penalties issued by OCR:

- Aetna: $1 million[3] for HIPAA violations related to HIV medication information disclosure in a mailing.
- City of New Haven, Connecticut: More than $200,000[4] related to non-restriction of access for a terminated employee to ePHI systems.
- Specifically related to the HIPAA Right of Access Initiative, in October, OCR announced two related settlements, one with Dignity Health, dba St. Joseph's Hospital and Medical Center, for $160,000[5] regarding issues meeting a patient representative's requests for records, and $100,000[6] for New York Spine, regarding issues with timely fulfilling a patient request for PHI.

Interestingly, while we have seen an uptick in OCR investigations and cyber threats, settlement costs aren't increasing at the same rate. That may be due, in part, to that investigation and settlement timeline mentioned earlier where cases settled today are likely to have originated years before the pandemic.

Breaches and third-parties

We mentioned earlier that if you're a covered entity and you discover a breach, you have reporting requirements to individuals and depending on the size of the breach, also to OCR and the media. It's important to remember to keep documentation of how you made these notifications as they may be required as part of the OCR investigation.

As part of your HIPAA security and privacy practices, be sure to have written policies about breach notification procedures in place and ensure that your employees are educated about what they must do regarding unauthorized disclosures, including how your organization handles employees who do not implement your required policies and procedures.

3 https://www.hipaajournal.com/aetna-1-million-hipaa-fine-for-data-breaches/

4 https://www.healthcareitnews.com/news/aetna-city-new-haven-hit-ocr-fines-after-data-breach

5 https://www.hipaajournal.com/ocr-imposes-160000-penalty-on-healthcare-provider-for-hipaa-right-of-access-failure/

6 https://www.hipaajournal.com/ocr-announces-9th-financial-penalty-under-its-hipaa-right-of-access-initiative/

© Clearwater | All Rights Reserved | 14.3

In addition to your internal policies, procedures, training, and follow up, don't forget about your responsibilities for PHI as it relates to business associates.

As we have seen with the adoption of more electronic patient health information records and portals—and especially in light of the rapid and increased use of telehealth during the pandemic, more and more organizations now rely on third-parties for services. That can be anything from a software as a service (SaaS) that runs your portal to mobile applications that give patients ePHI records on the go.

If your business associate has a breach of your PHI, then you're still ultimately responsible for the PHI privacy and security.

First-party and third-party access

Not only do the HIPAA privacy and security rules still apply to your third-parties, but so does right to access, so, if you're using third-parties for these services, you'll still need to ensure your patients can access their ePHI in the form and formats they're requesting.

The format and usability areas also shine a light on first-party (the patient/individual's) right to access and should also be noted here. For example, let's say your organization has moved to a digital-only records system, but your patient requests paper copies of PHI. Do you have to comply with the paper request? Yes.

When it comes to electronic health records (EHR) and other related technologies, you need to ensure seamless access for patients to their records, and that's more than just access to your patient portal. That could include, among other formats, the paper request we just mentioned.

Unfortunately, many organizations have institutional roadblocks that can prohibit or delay such requests. Sometimes that's a result in a misunderstanding of your organization's policies and procedures so team members may not realize what they have to provide or there may be confusion about related fees. When this happens and there is a untimely delay in release of records or out-of-scope fees, the individual can file a complaint with OCR, which may trigger an investigation and related penalties and corrective actions.

© Clearwater | All Rights Reserved | 14.3

Determining disclosure

When a covered entity discovers a breach, it generally presumes that PHI has been breached with impermissible use or disclosure, unless it can determine through a risk assessment that there is a "low probability" of PHI compromise.

Here are the four issues[7] [8] that must be

determined through the risk assessment:

1. What is the nature and extent of the PHI, including identifiers and re-identification likelihood?

7 https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
8 Data based on Clearwater proprietary research. Available upon request.

Recent OCR Enforcement Penalties

Aetna:

$1M for HIPAA violations

City of New Haven, CT:

More than $200,000 related to non-restriction of access for a terminated employee to ePHI systems.

Dignity Health:

$160,000 regarding issues meeting a patient representative's requests for records

New York Spine:

$100,000 for untimely fulfillment

© Clearwater | All Rights Reserved | 14.3

2. Who was the unauthorized person who used the PHI or to whom the disclosure was made?
3. Was the PHI acquired or viewed?
4. To what extent has the PHI risk been mitigated?

There are also a few exceptions to what defines a breach. For example:

- A covered entity employee or a business associate unintentionally accesses, acquires, or uses the PHI in good faith and within authority scope
- A person authorized to access PHI has an inadvertent disclosure
- If the authorized covered entity or business associate individual believed in good faith the person to whom the disclosure was made could not retain that PHI

The importance of risk analysis

If we look at OCR enforcement actions related to ePHI, in 88% of these cases, the most significant causes of insufficiency or lack of compliance are related to risk analysis.

Basically, that means that in almost 90% of those instances, organizations haven't done OCR quality risk analysis.

Before the height of the pandemic, OCR Director Roger Severino[9] pointed out that, "There are a lot of entities that are not doing the basic steps to make sure they have proper, for example, cybersecurity protections in place. They're not doing the comprehensive risk analyses on the front end."

That certainly brings front-of-mind, why? Why would organizations, knowing there is increasing numbers of breaches and increasing numbers of enforcement settlements not tackle these basic practices?

For many, it's because they see risk analysis as too challenging, so they just follow a security checklist or some other more basic means of assessing risk —even though there's no reduction or elimination of responsibility in this approach. That's because when OCR begins its investigation, thinking back to those culpability tiers and penalties discussed earlier, one of the first questions an investigator is likely

9 https://digital.mwe.com/27/7458/landing-pages/hipaa-boss-sees--low-hanging-fruit--ripe-for-enforcement---law360.pdf

© Clearwater | All Rights Reserved | 14.3

to pose will be related to risk analyses prior to the breach. And it may not just be your latest risk analysis they'll want documentation for. Because you're expected to document these analyses for at least six years, you may be required to provide your documentation for that entire timeframe. If you haven't done one–or haven't conducted recent analyses–your culpability could increase, as could the severity of your penalties.

Risk analysis versus gap analysis

Another challenge for many organizations is a lack of understanding about the differences between a risk analysis compared to a gap analysis. Some organizations may enter into an OCR investigation believing they're successfully completed a risk analysis, when in actuality all they've tackled is a gap analysis.

Here's a simple way to look at it. With HIPAA you have a list of compliance requirements. In a gap analysis, you can list out all of those requirements, evaluate which ones you're successfully meeting, and where you uncover deficiencies, you find your gaps.

A risk analysis is more detailed. While you may end up with the similar results—uncovering gaps—the risk analysis will actually reveal which controls or measures you should implement to mitigate those gaps. A risk analysis will also help you determine your most critical systems and applications and determine which issues cause the greatest risks for your organization so you have a better understanding of what you should address first.

While risk analyses can be challenging for organizations of all sizes, larger enterprises often struggle because of the vast amount of data, systems, and related applications and technologies used that may create, transmit, process, or store PHI. While they might have an understanding of risks, they may struggle to implement efficient processes that mitigate or eliminate that risk for the entire organization and all of its data. Many feel like addressing the full gamut of risks is just too vast and they don't know where to start or what they're required to do.

It's even further complicated by increased reliance on third-party vendors and their related risks, but it's a component that can't be overlooked, especially because in the two years prior to 2020, data breaches that originated with third-parties increased nearly 35%[10].

10 https://www.darkreading.com/attacks-breaches/third-party-breaches---and-the-number-of-records-exposed---increased-sharply-in-2019/d/d-id/1337037

© Clearwater | All Rights Reserved | 14.3

So where do you begin? How do you do a risk analysis for your organization and then how do you replicate your risk standards and expectations through your supply chain?

OCR risk analysis guidance

OCR offers risk analysis guidance to help organizations with HIPAA compliance, which is the first step in complying with the HIPAA Security Rule. A great starting point is the National Institute of Standards and Technology's (NIST) Risk Management Framework. This framework is a nationally recognized set of standards, considered best practices, for developing information security practices. You can even map (or crosswalk) HIPAA Security Rule requirements with the NIST framework controls for risk assessments and cybersecurity.

OCR's guidance points out that although federal agencies are required to meet NIST guidelines, other organizations can benefit from these standards to secure ePHI, beginning with risk analysis.

Risk analysis tools

Another useful tool for successful and meaningful risk analysis is to consider implementing a risk analysis solution that can help you automate processes and give you a comprehensive view into all of your gaps, while helping you meet compliance mandates. For example, Clearwater's IRM|Analysis® can help you adhere to OCR's risk management guidance and meet HIPAA Security Rule requirements. Organizations that use IRM|Analysis (or in consultation with Clearwater) to submit risk analyses to OCR have a 100% success rate.

Here's are some of the critical tasks you can simplify with IRM|Analysis:

- Discover all your ePHI systems and where they're located
- Review and analyze all existing documents
- Document existing controls
- Discover gaps and deficiencies
- Uncover threats and vulnerabilities related to ePHI
- Risk identification and classification
- Determine risk levels based on impact and likelihood based on NIST 800-30
- Comprehensive insight into your controls and policies in a single dashboard

© Clearwater | All Rights Reserved | 14.3

Need help developing your risk management program or want to know more about how a risk analysis can help decrease your chances of HIPAA-related breaches? Check out our on-demand webinars that tackle a variety of risk analysis and HIPAA compliance topics. You can find a complete list at clearwatercompliance.com/on-demand-videos.

© Clearwater | All Rights Reserved | 14.3

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact

© Clearwater | All Rights Reserved | 14.3