

Key Data Points from HHS Office of Civil Rights Reports on HIPAA Breaches



CJ Wolf MD, CHC, CPC, CCEP, CIA



In February 2023, the HHS Office for Civil Rights (OCR) submitted two reports to the U.S. Congress on HIPAA and Breaches (see: <https://www.hhs.gov/about/news/2023/02/17/hhs-office-civil-rights-delivers-annual-reports-congress-hipaa-compliance-breaches-unsecured-protected-health-information.html>).

The two reports are titled:

- *HIPAA Privacy, Security, and Breach Notification Rule Compliance*
- *Breaches of Unsecured Protected Health Information*

It's always a good idea to see what enforcement agencies submit to their bosses – in this case, the Congress.

In the press release, OCR Director Melanie Fontes Rainer said, "The health care industry is one of the most diverse industries in our economy, and OCR is responsible for enforcing the HIPAA Rules to support greater privacy and security of individuals' protected health information." The reports offer summary data and narratives for the calendar year 2021.

HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE COMPLIANCE

This report includes interesting data and subsequent explanations.

For example, OCR reports they did not perform any proactive audits in 2021 "due to a lack of financial resources." Even enforcement agencies have to be selective in their work, just like compliance departments embedded in health care organizations around the country.

According to the report, the number of HIPAA complaints received by OCR has increased 39% from 2017 to 2021. OCR stated this is one of the key reasons the agency is experiencing severe strain on their limited staff and resources. Specifically, they told Congress, "This lack of necessary funding limits OCR's HIPAA enforcement activities during a time of substantial growth in cybersecurity attacks to the health care sector."

In 2021, OCR received 34,077 new complaints of HIPAA violation allegations, representing a 25% increase from the prior year. Of the 34,077 complaints, OCR resolved 26,420. They resolved 78% (20,661) before even beginning a formal investigation. Another 16% (4,139) were resolved by providing technical assistance

rather than an investigation. When it came to investigations, 3% (741) of covered entities or business associates took corrective action.

Most compliance professionals see the headlines related to significant cases. In this context, OCR resolved 13 complaints with formal resolution agreements and corrective action plans. The monetary settlements totaled \$815,150, with civil monetary penalties totaling \$150,000.

OCR also completed 573 compliance reviews. 83% of the time they required the entities to either take corrective action or pay a civil monetary penalty. Two of their compliance reviews resulted in formal agreements or corrective action and payments totaling \$5,125,000.

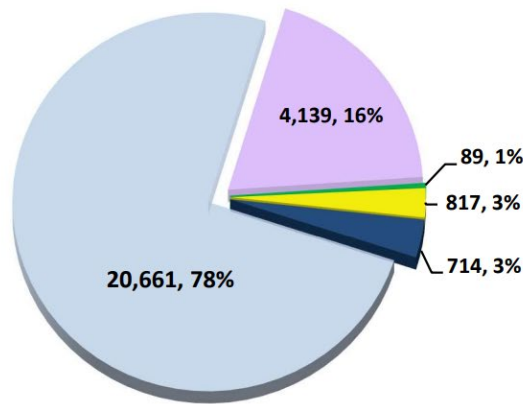




SUMMARY OF COMPLAINTS AND COMPLIANCE REVIEWS

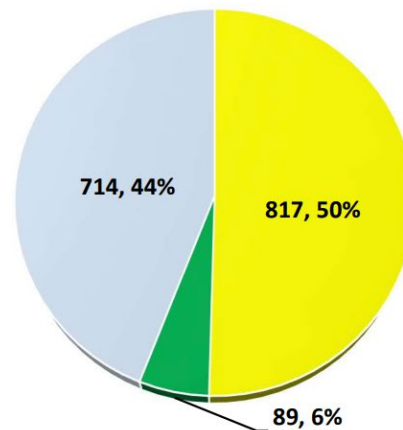
Year	Complaints Received	Compliance Reviews Initiated	Under 500 Breaches Reported	500+ Breaches Reported	% Change in complaints received	% Change in Compliance Reviews Initiated	% Change in Under 500 Breaches Reported	% Change in 500+ Breaches Reported
2021	34,077	674	63,571	609	25% increase	-10% decrease	-4% decrease	-7% decrease

COMPLAINT INVESTIGATIONS AND RESOLUTIONS, NUMBER OF CASES CLOSED, AND TYPE OF CLOSURES JANUARY 1, 2021 THROUGH DECEMBER 31, 2021



TOTAL RESOLUTIONS: 26,420
 ■ Resolved after Intake and Review
 ■ Pre-Investigational Technical Assistance
 ■ Post-Investigational Technical Assistance
 ■ Investigated: No Violation
 ■ Investigated: Corrective Action Obtained

Figure 1



TOTAL INVESTIGATIONS: 1,620
 ■ Investigated: No Violation
 ■ Post-Investigational Technical Assistance
 ■ Investigated: Corrective Action Obtained

Figure 2

BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

The second report submitted to Congress focused on breaches of unsecured Protected Health Information (PHI).

OCR offered the definition of a “breach” as the “acquisition, access, use, or disclosure of PHI in a manner not permitted by [the HIPAA Privacy Rule] which compromises the security or privacy of the PHI” and provided the regulatory reference 45 CFR § 164.402.

Compliance professionals familiar with the Breach Notification Rule also know there are exceptions if the covered entity or business associate can demonstrate a low probability that the PHI has been compromised based on a risk assessment.

Such a risk assessment must address at least the following factors:

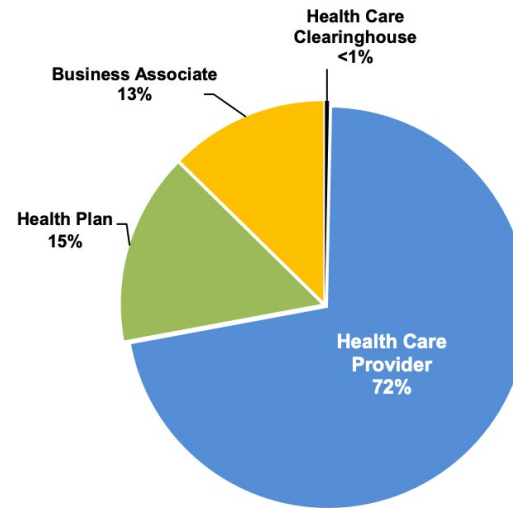
1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made.

3. Whether the PHI was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

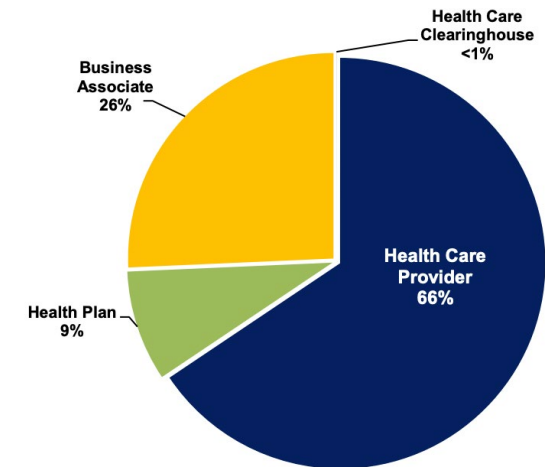
OCR received 609 notifications of breaches affecting 500 or more individuals. This represents a 7% decrease in the number of reports compared to 2020. The number of individuals affected by these breaches totaled approximately 37,182,558. The most reported category of breaches? You guessed it...hacking.

OCR is also required to report breaches affecting less than 500 individuals. For this category, OCR received 63,571 reports with the number of individuals affected by these types of breaches totaling 319,215.

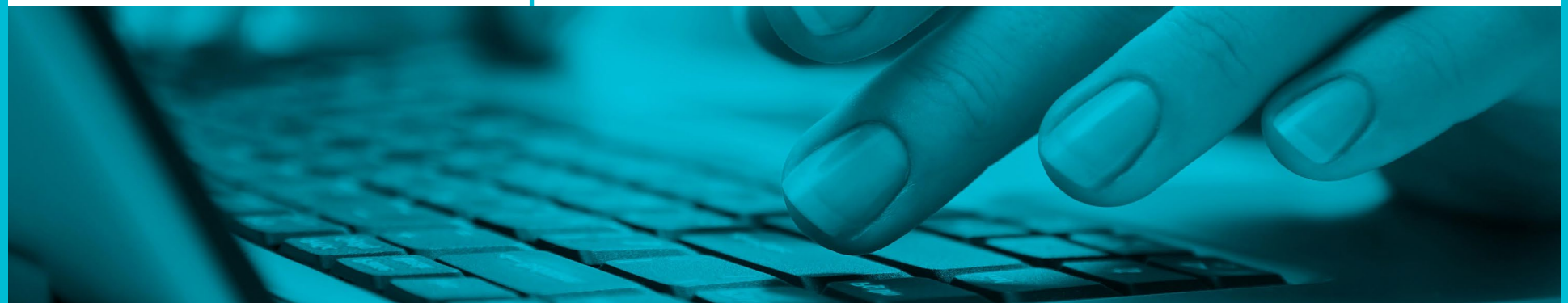
Some of the more interesting data shared about breaches included the following:

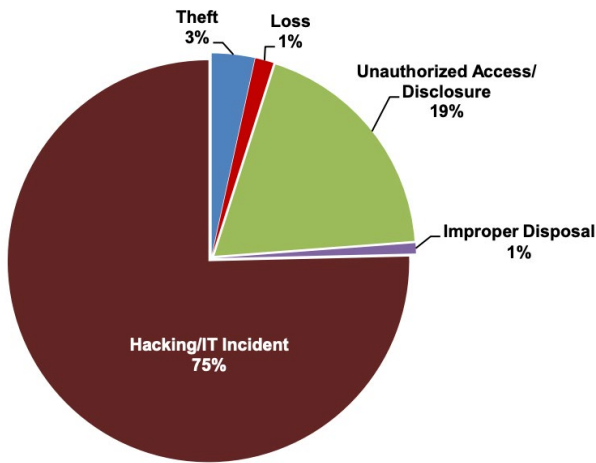


Breach Reports of Unsecured PHI Affecting 500 or More Individuals in 2021 by Percentage of Reports Received by Entity Type

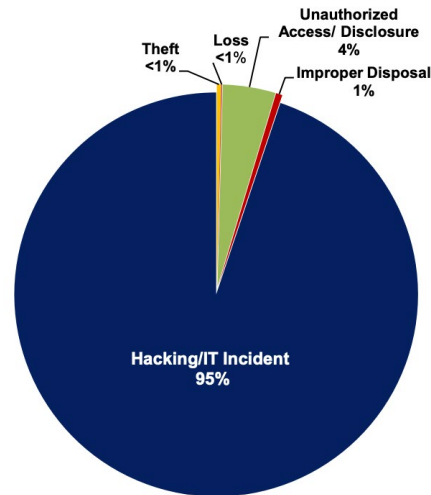


Breach Reports of Unsecured PHI Affecting 500 or More Individuals in 2021 by Percentage of Individuals Affected by Entity Type





Breach Reports of Unsecured PHI Affecting 500 or More Individuals in 2021 by Percentage of Reports Received by Type of Breach



Breach Reports of Unsecured PHI Affecting 500 or More Individuals in 2021 by Percentage of Individuals Affected by Type of Breach

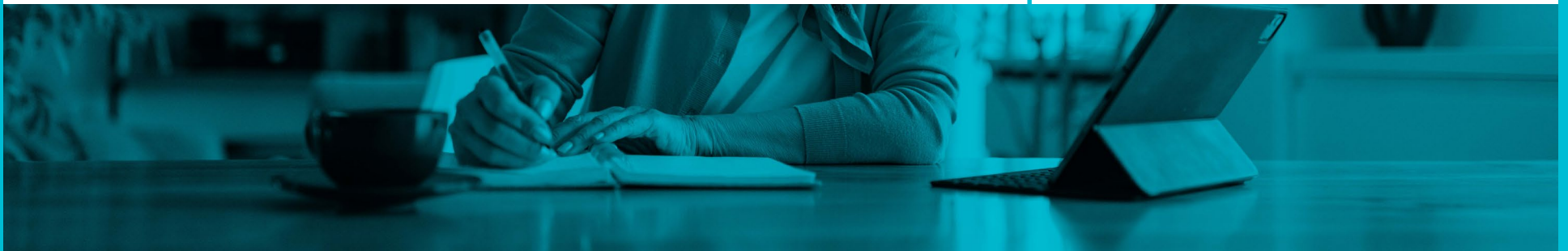
CONCLUSION

It is always interesting to study the overall statistics of HIPAA violations, allegations, and breaches. The data tells us much about some of the greatest risks facing covered entities and business associates.

If your whistle has been whetted and you are interested in reading even more detail from the reports, you can read them here:

OCR's 2021 Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance may be found at: <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html>

OCR's 2021 Report to Congress on Breaches of Unsecured Protected Health Information may be found at: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html>





CJ Wolf

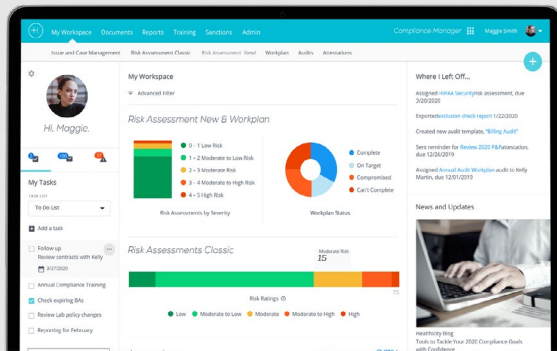
MD, CHC, CPC, CCEP, CIA

CJ Wolf is a healthcare professional with more than 20 years of experience in hospital and physician revenue cycle, practice management, compliance, coding, billing, and client services. He has provided healthcare consulting and solution services to hospitals and physician organizations throughout the country.



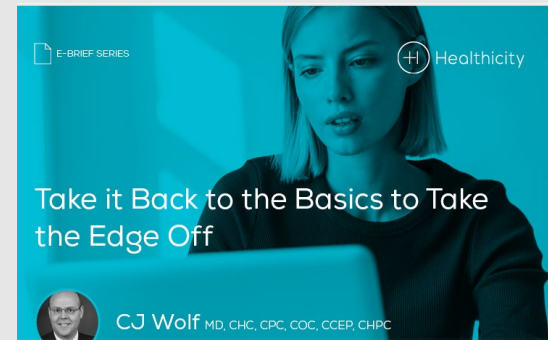
For more on Healthicity's [Compliance Services and Solutions](https://healthicity.com/compliance), please visit healthicity.com/compliance or call 877.777.3001

COMPLIANCE MANAGER



WATCH ON-DEMAND DEMO

RESOURCE CENTER



EXPLORE FREE RESOURCES