PROTENUS®

protenus.com

Contents

Introduction

In 2021, the healthcare industry faced rising supply costs, higher salaries, and critical staffing shortages exacerbated by COVID-19 on top of the continued challenge of employee retention and satisfaction, patient safety, and organizational success. Although the availability of vaccines provided some relief on the coronavirus front, hospitals and health systems across the country found themselves swamped with patients, severely short-staffed and at times lacking critical supplies. Although bad actors have relentlessly exploited healthcare's weak spots for years, continuous disruption made the industry an even bigger target in 2021. Greater reliance on virtual care delivery and remote work exacerbated the vulnerabilities of sensitive patient data while hackers deployed more sophisticated tactics.

"The healthcare sector has been a main target of cyberattacks," California Attorney General Rob Bonta wrote in a late August bulletin urging healthcare entities to fulfill their breach reporting obligations. "Across the nation, cyberattacks on the healthcare sector [have] interrupted service delivery and patient care, and eroded patient trust."

The bulletin put in perspective that while a record number of data breaches were reported to the federal government in just the first half of 2021, the volume and impact of breaches continue to be underreported overall, and underrepresented to the public. This retrospective report examines the extent of all known health data breaches in 2021, going beyond those that are reported to the government to provide the most complete picture possible – though gaps in detection and reporting mean the true impact of incidents is likely even greater. The analysis also explores the actions taken to remedy incidents, in the hopes of enabling healthcare organizations to take more effective, proactive protections going forward.

Overview of 2021 Findings

Our analysis is based on 905 health data breaches reported to HHS, the media, or some other source during 2021 (Figure 1). As in past years, details on the number of records affected were not available for each incident, but for the 700 incidents where the information was known, 50,406,838 patients were impacted (Figure 2). Readers should refer to the Methodology section at the end of this report for detailed information on how data was coded and compiled, but it should be understood that the Breach Barometer uses a coding system different from that used by HHS in its breach reporting tool. The coding system for this report distinguishes healthcare employee events from external actor incidents, and it encompasses incidents involving health-related or medical information about U.S. residents or citizens — whether or not it impacts a HIPAA-covered entity. Additionally, whereas the HHS breach portal may show multiple entities reporting the same incident, the Breach Barometer counts those multiple reports as a single new incident.

Figure 1 - Total known incidents, 2021 health data breaches by month

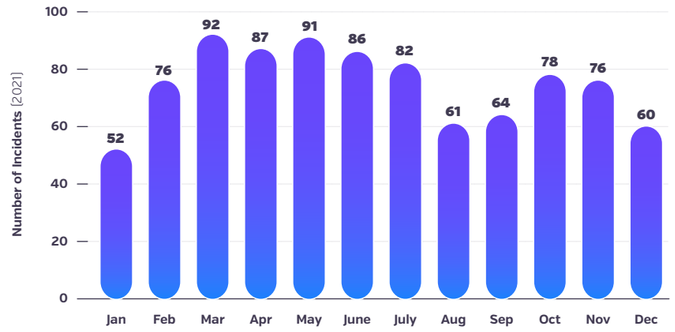


Figure 2 - Total incidents, 2016-2021 health data breaches

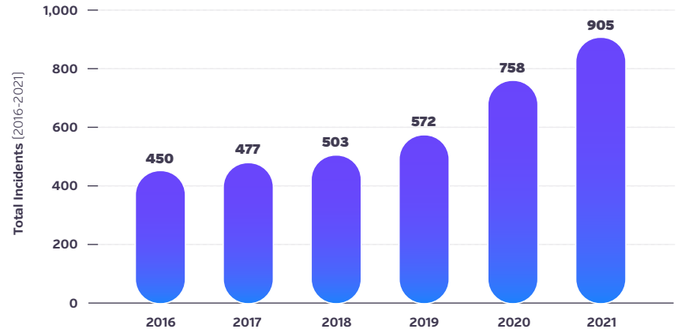
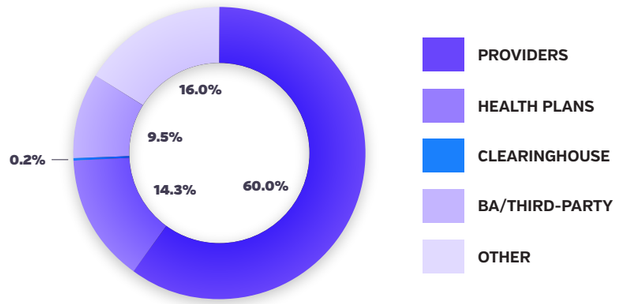


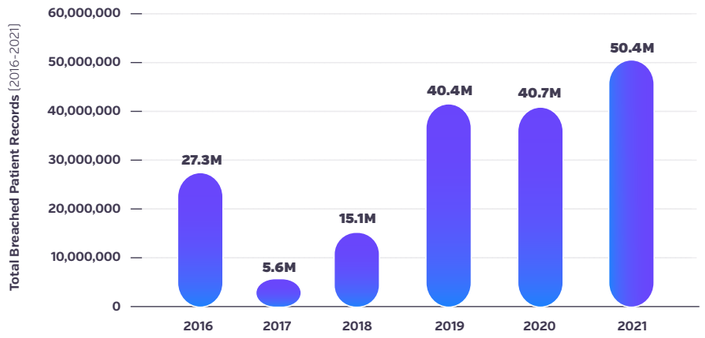
Figure 3 - Types of entities that reported or disclosed incidents, 2021 health data breaches



The increasing sophistication of hackers is outpacing the adoption of new protections by the healthcare industry, and providers in particular are suffering for it. While hospitals' attention has been occupied by persistent staffing shortages, supply chain disruptions, and other changes related to COVID-19, their outdated methods for detecting improper access are creating a large blindspot.

Year over year, the number of breaches reported increased 19%: there were 905 reported in 2021, compared to 758 in 2020. The number of patient records affected in 2021 was up 24% over 2020, when a total of 40,735,428 patient records were compromised in just 609 incidents where this measure of breach impact was known. However, it is important to note that the total volume of patients impacted cannot be known until investigations have been completed, and the true number is undoubtedly higher.

Figure 4 - Total breached patient records, 2016-2021 health data breaches



The increasing sophistication of hackers is outpacing the adoption of new protections by the healthcare industry, and providers in particular are suffering for it (Figure 3). While hospitals' attention has been occupied by persistent staffing shortages, supply chain disruptions, and other changes related to COVID-19, their outdated methods for detecting improper access are creating a large blindspot. The threat is concerning enough that in late October, the HHS Office for Civil Rights advised healthcare organizations to re-evaluate the use of legacy IT systems and devices, noting their increased vulnerability to cyberattacks.

2021 Largest Health Data Breaches

Month	Organization Type	Type of Breach	Number of Affected Patient Records
January	Business Associate	Hack	3,500,000
February	Business	Hack	1,474,284
March	Provider	Ransomware	134,906
April	Provider	Ransomware	499,779
May	Provider	Unknown*	3,253,822
June	Provider	Hack	2,413,553
July	Business	Hack	1,210,688
August	Provider	Hack	1,515,918
September	Govt provider	Hack	500,000
October	Provider	Hack	656,047
November	Provider	Hack	2,102,436
December	Provider	Ransomware	750,750

Figure 5 - Largest incidents, 2021 health data breaches

*The affected entity reported the breach as an "insider wrongdoing" case, but without clarity as to whether their definition matches the definition used within this analysis, we classified the breach as "unknown" in nature.

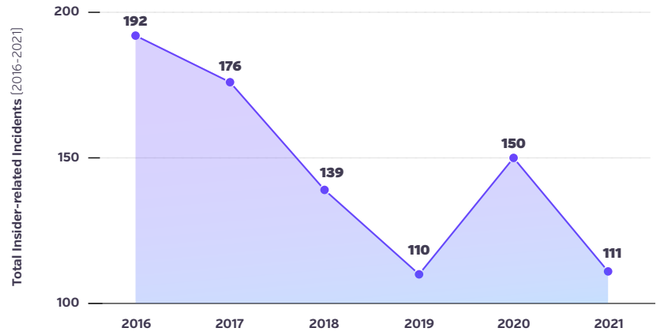
The Single Largest Breach

The single largest breach reported in 2021 (Figure 4) was the result of a hacking incident involving the IT business associate of a children's health plan. The Tallahassee, Fla.-based health plan, which caters to children who are not Medicaid-eligible and offers year-round enrollment, announced the hack of its website in January. The incident affected as many as 3,500,000 individuals who applied for health insurance between 2013 and December 2020. An investigation into the breach revealed hackers had exploited vulnerabilities in the health plan's website that the web hosting provider hadn't patched or addressed. This allowed attackers to access information including full names, birth dates, email addresses, phone numbers, addresses, Social Security numbers, financial information, familial relationships and secondary insurance data. There was evidence that applicant addresses had been tampered with, and although there was no concrete evidence that hackers had exfiltrated the exposed data, affected individuals were advised to take measures to protect their identities.

Insider Incidents Account for More Than 1 in 10 Breaches

In this analysis, each insider incident is classified as either insider-error or insider-wrongdoing. The former includes accidents and human error, whereas insider-wrongdoing includes employee theft of information, snooping in patient files, and otherwise intentionally violating the law or organizational policy.

Figure 6 - Total insider-related incidents,, 2016-2021 health data breaches



With 111 new insider incidents recorded throughout the year (Figure 6), insiders were responsible for 12% of the total number of breaches in 2021. The number of breaches categorized as insider incidents was down from 150 in 2020, when sensitivity around Covid-19 diagnoses may have driven a spike in either insider curiosity or organizational detection of impropriety, which has since subsided. The number of insider-related incidents remained in line with the pre-pandemic volume reported in 2019, when there were 110.

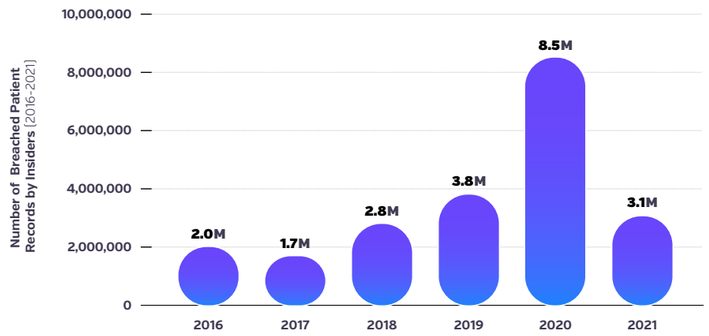
While our analysis shows an overall decrease in insider-related incidents, it is necessary to bear in mind that insider incidents that occurred throughout the year may have yet to be reported for various reasons including: they have not yet been discovered; they have been discovered but law enforcement action has delayed notification; or the affected entity is not aware of or adhering to reporting obligations.

Additionally, it is important to recognize that insider behavior can and often does give outsiders a foothold for improper access to patient data, in incidents ultimately reported as hacking-related. For instance, if a healthcare worker is tricked into clicking a malicious link that enables hackers to take control of millions of records, the incident may be reported as a ransomware attack, but insider error is certainly a contributing factor. Therefore, insider behavior may have provided a foothold for many of the hacking incidents that accounted for the majority of breaches in 2021, making the overall number of insider incidents a vast under-representation of the extent to which insider behavior contributes to breaches. Whether it's a simple employee error giving hackers access to patient data or a nefarious entity

successfully enlisting a healthcare worker's help, the vulnerabilities that insider behaviors can create should not be ignored.

Even when insiders mishandle patient data in ways that they believe will help them perform their job better, it may jeopardize patient trust and cost the organization both financially and reputationally. For example, a Florida health plan discovered in June 2021, while reviewing a former employee's email account, that the individual had sent emails containing internal documents to their personal email in violation of organizational policy. Although the employee was within the scope of their professional duties in accessing these documents and the beneficiary information they contained, their policy violation put 48,344 individuals at risk of identity theft and fraud.

Figure 7 - Number of breached patient records by insiders, 2016-2021 health data breaches



As in past years, we conclude that the overall number of patient records compromised by insider incidents in this analysis does not fully capture how many were actually breached by insiders during the year. Just 90 of the year's 111 insider incidents had available information on the number of records affected. That portion of insider incidents still did extensive damage, compromising a combined total of 3,056,074 patient records, or 6% of all patient records breached throughout the year (Figure 7). On average, each insider incident during the year exposed more than 33,956 records.

Hacking Incidents Climb for 6th Consecutive Year

With a total of 678 newly disclosed and unique hacking incidents occurring throughout the year, 2021 marked the sixth consecutive year that hacking incidents were on the rise (Figure 8). Hacking incidents, which include ransomware and malware incidents, phishing and email incidents, or other kinds of attacks by external actors, accounted for approximately 75% of all breaches in 2021. Hacking during the year affected 43,782,811 patient records in total — or 64,576 per incident, on average. This category, including external hackers and insider events that opened the doors for them, represents 87% of all breached records during the year, illustrating the enormous damage that hackers cause.

Figure 8 - Total hacking incidents, 2016-2021 health data breaches

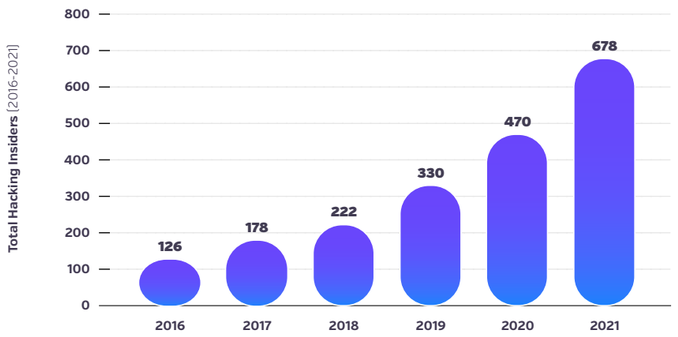


Figure 9 - Total hacking incidents by quarter, 2021 health data breaches

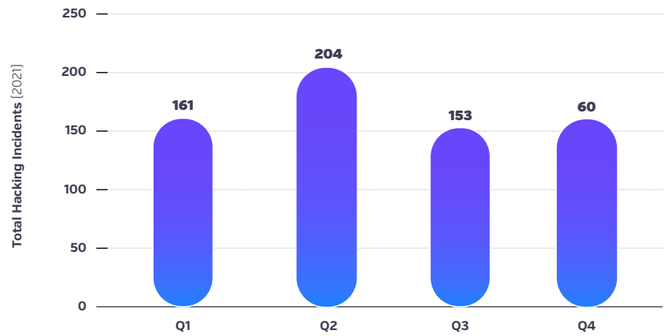
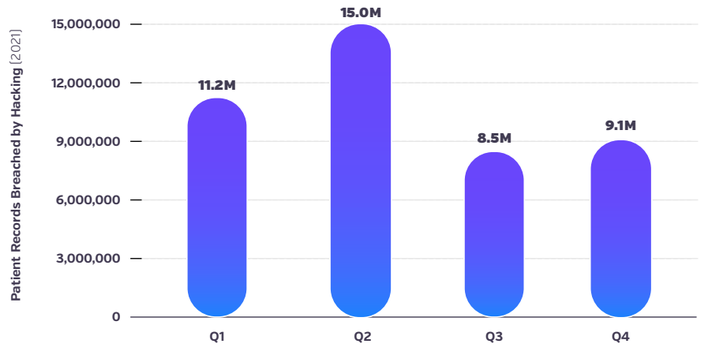


Figure 10 - Patient records breached by hacking, 2021 health data breaches



When examining the frequency of hacks throughout the year, it was found that they were occurring at a fairly steady pace, with at least 150 hacking incidents being reported each quarter (Figure 9). The second quarter was the worst for hacking-related incidents, with a total of 204 from April through June affecting nearly 15 million records. After the spike in incidents in Q2, numbers decreased and leveled off over the third and fourth quarters, returning to roughly the same volume observed in Q1. While any reduction in the volume of incidents is promising, it may have simply been the result of law enforcement actions causing criminal groups to stay off the radar — temporarily. In 2022, we anticipate further increases as these groups rebrand and re-emerge.

Just as hackers took advantage of a pandemic-strained system in 2020, the same remained true during the course of 2021. In-hospital patient volumes moved toward 2019 levels but virtual care delivery was also highly utilized — all while the healthcare workers needed to keep everything running efficiently became increasingly scarce. The tumultuous conditions, including the reallocation of resources from administrative and compliance functions to direct patient care, were ideal for hackers to succeed at obtaining patient data.

In one notable instance from 2021, a ransomware incident exposed the files of nearly 1.6 million health system patients. These sensitive patient files were available on the dark web for several months (and were being reported on by media for several months) before the Indiana-based organization publicly acknowledged the exposure. Although health system officials commended the quick action staff took to shut down the IT network and deploy EHR downtime procedures, the attack came just as Indiana's Delta COVID-19 surge was taking off, creating further strain on staff and patients at the worst possible time.

Getting ahead of sophisticated hackers in an industry marked by continuous disruption will require healthcare organizations to conduct thorough and honest risk assessments, provide effective employee training and ensure ongoing education. Education should also be delivered on a targeted, on-the-spot basis for healthcare employees found to be improperly handling patient data, so as to prevent future misuse of privileged access, including accidentally falling victim to phishing attempts. Automation and artificial intelligence have tremendous potential to facilitate a proactive approach to protecting patient data in these and other circumstances, allowing for quick, informed intervention and targeted education where appropriate. By investing in technologies with these critical functionalities, thoroughly

vetting business associates to ensure top-of-the-line security protections are in place, and leveraging up-to-date, informative resources from HHS, healthcare organizations can position themselves to offset the increasing costs of worsening data breaches.

"Inefficient legacy systems pose a serious risk to healthcare infrastructure security as a whole," said Michael Archuleta, Chief Information Officer for Colorado-based Mt San Rafael Hospital, at Xtelligent Healthcare Media's Privacy and Security Digital Summit in April 2021. "We need to implement intelligent security that focuses on endpoint devices, assessment management, as a whole, to create a hawkeye view of what we have in our environments."

Other Types of Breaches

Aside from hacking and insider incidents, there were also 32 theft-related breaches in 2021. Information was available for 28 of those incidents involving theft, and together, they affected 110,655 patient records. There were 11 identified incidents of lost or missing records, and only one did not have information available on records impacted. This category of incidents potentially exposed the information of 30,922 individuals.

While most of the breaches included in this report involved digital data, we did not neglect to compile data from breaches involving other formats. For 2021, there were 48 incidents involving paper records (Figure 12), and 47 of those which had the relevant data affected 176,496 patients.

Finally, there were 73 incidents that could not be categorized due to insufficient information. In the 69 uncategorized incidents for which the numbers were available, a total of 3,426,376 records were affected.

Figure 11 - Type of incidents, 2021 health data breaches

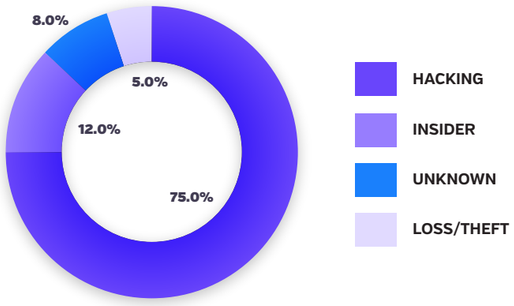
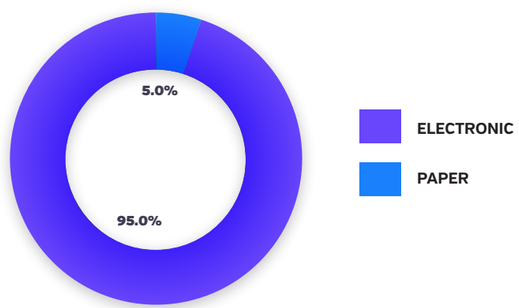


Figure 12 - Paper vs. electronic records, 2021 health data breaches

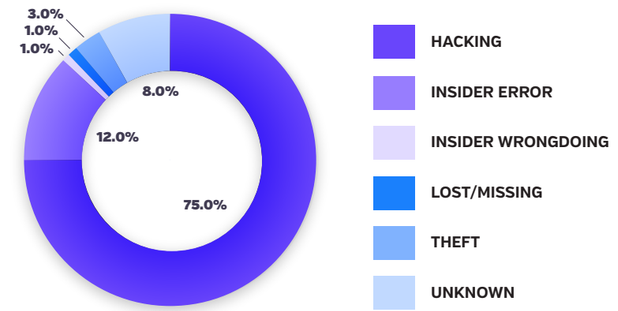


Business Associates Responsible for 20,986,509 Records Breached

The number of incidents involving a business associate (BA) or third party increased slightly from 2020, but nearly doubled the total in 2019. BAs were affected by a combined 146 of these incidents in 2021 (Figure 13).

Of the breaches involving BAs, the majority — 109 incidents, or 75% — were a result of hacking. Bad actors were happy to exploit errors involving BAs, such as leaving Remote Desktop Protocol enabled and client logins exposed in plain text. Supply chain attacks, such as one reported by DataBreaches.net, remind us that a hospital's systems and functioning can potentially be severely disrupted if a vendor does not properly secure client information.

Figure 13 - BA/third-party involvement, 2021 health data breaches



The second biggest cause of BA-related incidents was insider behavior, with 17 insider-error incidents and two insider-wrongdoing incidents. The insider incidents' major contribution to BA incidents for the year serves as a reminder that these entities have their own insiders whose human errors or malicious actions put patient data at serious risk. With ransomware gangs ramping up recruitment of healthcare insiders to carry out attacks, it is critical that hospitals and health systems ensure that both they and their business partners have measures in place to immediately identify any improper access to patient data, no matter who it stems from.

Even with nearly 21 million patient records affected by BA-involved incidents in 2021, that number is undoubtedly a significant underestimate as we did not have full reports for many of these incidents. Moreover, the average BA-involved incident affected far more individuals than other kinds of breaches, with an average of 143,743 records compromised. It should be kept in mind, though, that the number of patient records affected varies greatly from incident to incident, with the year's largest breach affecting 3.5 million.

Breaches Left Undiscovered for Average of 132 Days

Figure 14 - Average number of days from breach to discovery, 2021 health data breaches

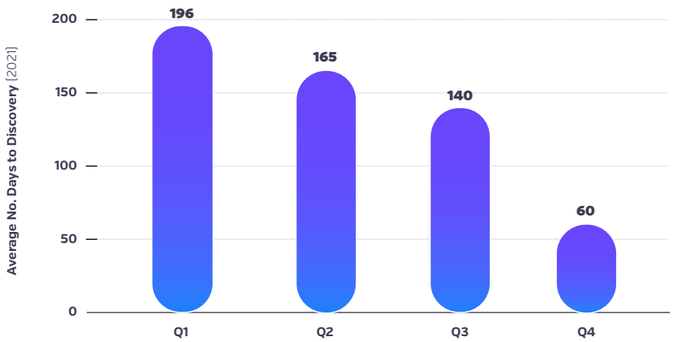
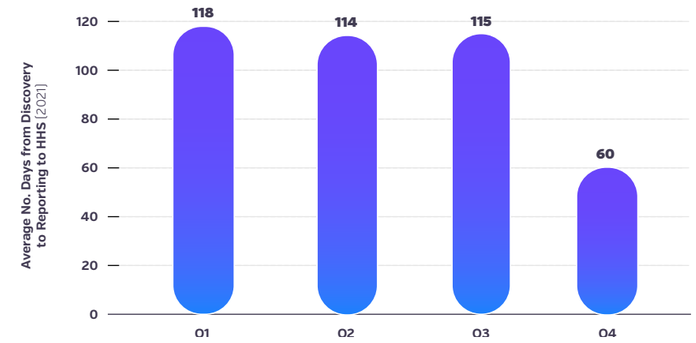


Figure 15 - Average number of days from discovery to reporting to HHS, 2021 health data breaches



When examining all incidents with relevant data in 2021, on average, 132 days passed between the time a breach occurred to the time it was discovered (for BA-involved incidents, the "discovery date" is defined as the date that the third party first discovered the breach — not the date that they first informed the covered entity about it). This represents a decrease of nearly 30% from 2020, when the average time to discovery was 187 days. The average time from breach to discovery is important to point out because it gives an indication of how long patient data can be misused before organizations even realize it has been exposed and take remedial action. The median time it took to discover a breach was just 20 days, but it should be noted that there were a wide range of time frames for discovery throughout the year. The shortest time to discovery was one day, and the longest was more than a decade.

Once a breach was discovered in 2021, the average time that elapsed before it was disclosed to HHS, the media, or other sources was 118 days, using the arithmetic mean. This means organizations are taking much longer to disclose incidents than they were just a year ago, possibly a result of continued pandemic-related staffing and time constraints, but alarming nonetheless. In 2020, the time between discovery and reporting was nearly 40% shorter, at 85 days.

The median disclosure time — which, unlike the mean, is not skewed by exceptionally large or small windows of time — was 62 for incidents identified in 2021. While this calculation includes entities not covered by HIPAA, it suggests that healthcare organizations are trying to adhere to HHS' required 60-day reporting window. However, alternative definitions of "discovery date" provide a way around that concrete number. While entities may hold off on notification until they understand more about an incident in question, it keeps patients in the dark at a critical time when they should be taking steps to protect themselves.

Organizations are taking much longer to disclose incidents than they were just a year ago.

It is important to note that the dataset for this analysis varies greatly from month to month, and data on disclosure timeframe wasn't available for every incident that occurred in 2021. Therefore, the smaller data set may not provide a full picture of reporting times throughout the year.

State Frequency

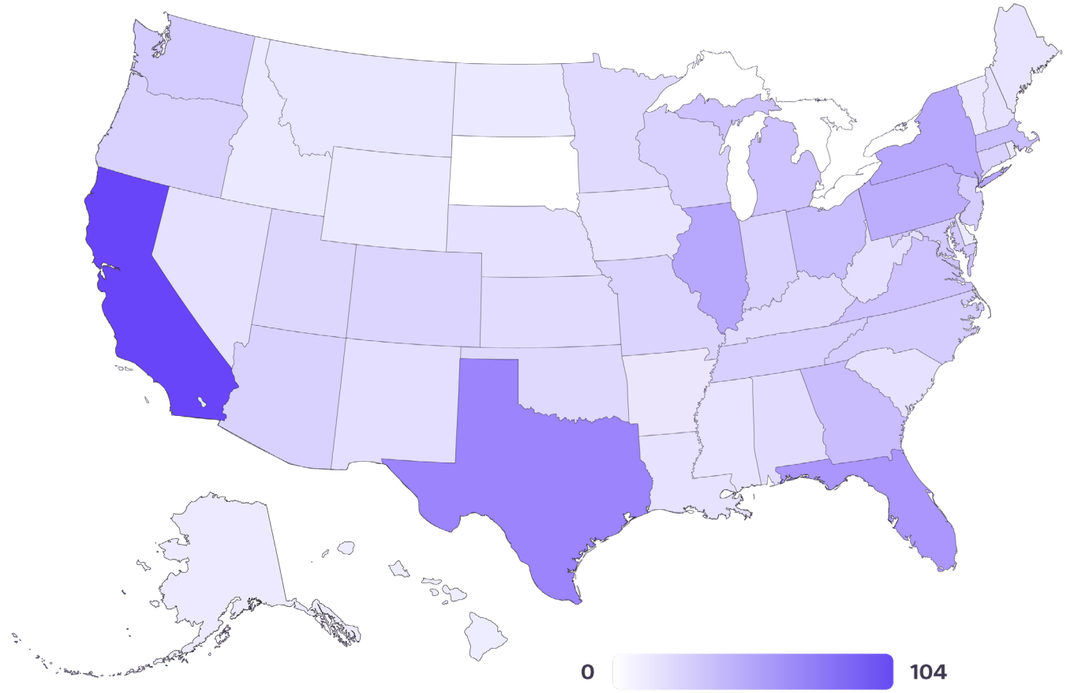


Figure 16 - Average number of days from discovery to reporting to HHS, 2021 health data breaches

Our analyses determined that 49 states (98%) were affected by data breaches in 2021 (Figure 16). Only one state did not have any reported breaches: South Dakota. California had the highest number of incidents with 104, followed by Texas with 65 and Florida with 54. Note that as in past years, each BA breach was assigned to the state in which the BA is headquartered, rather than the client's state. Therefore, Figure 17 shows the frequency where disclosed breaches originated, leading to an underestimate of how many reports and records were involved for each state.

Even with California tallying the most incidents for the second straight year, one state official felt compelled to issue a bulletin in August reminding healthcare providers and facilities to provide notice of breaches, after several went unreported. The broader implication is that in states where breach counts appear to be much lower, it is likely not because they are occurring with less frequency, but because they are going undetected or unreported. This map does suggest that some states have more businesses involved in breaches, and enforcement of good data security and notification practices could be improved.

Conclusion

In 2021, healthcare continued to see a concerning rise in hacking incidents and other major threats to patient data privacy. As the colossal industry moves toward greater reliance on technology, we can only expect these trends to worsen. Patient information is exceedingly vulnerable as threat actors sharpen their skills and exploit healthcare's outdated and ineffective breach protections, as well as the industry's beleaguered workforce, even going so far as to recruit healthcare insiders for help carrying out attacks. For healthcare organizations, this emerging threat only compounds the risk that naturally coincides with hundreds or thousands of workers' need to access large volumes of patient data throughout the course of their daily activities.

Patient information is exceedingly vulnerable as threat actors sharpen their skills and exploit healthcare's outdated and ineffective breach protections, as well as the industry's beleaguered workforce, even going so far as to recruit healthcare insiders for help carrying out attacks.

With the number of patients impacted and potentially harmed by data breaches nearly doubling from 2016, not a single potential opportunity for unauthorized access to patient data should be overlooked. While hacking incidents remain the leading cause of patient data breaches and warrant the extensive attention they receive from organizations, the media, and regulators, it is reckless to brush aside threats to patient data that come from insider mistakes or ill-intent — especially amid rampant burnout and a staffing crisis of historic proportions.

Industry experts have been warning for some time that healthcare breaches are a matter of "not if, but when." This sentiment drives home the urgency of ditching vulnerable legacy systems and prioritizing investment in real-time breach detection and prevention. Many hospitals and health systems have taken important steps to gain insight into how data moves through their organizations and where threats must be addressed, but the industry's room for improvement is undeniable. In 2022 and beyond, technology-powered visibility into patient data access will empower healthcare institutions to safeguard the sensitive patient data they house and to effectively mitigate organization-wide risk.

"The role of compliance has evolved significantly and moved past the basics. The need for more robust, data-driven compliance monitoring efforts are more necessary than ever before, especially in a time of constant change and the need to maximize efficiency in budgets."

– **Helenmarie Blake**, VP and Chief Compliance Officer and Privacy Offer, Nicklaus Children's Health System

About Protenus

The Protenus healthcare compliance analytics platform harnesses the power of artificial intelligence to audit every access to patient records for the nation's leading health systems, providing healthcare leaders full insight into how health data is being used, and alerting privacy, security, and compliance teams to inappropriate activity. Protenus helps our partner hospitals transition from a reactive posture to a proactive posture that focuses on risk reduction and prevention, better protecting their data, their patients, and their institutions. We are committed to innovation, determined to reduce risk, and focused on supporting our community of employees, customers, and ultimately, patients. Empowering healthcare to eliminate risk is at the heart of all we do. Protenus is a three-time winner of *Forbes'* Best Startup Employers, named one of *CBInsights'* Digital Health 150, named one of The Best Places to Work in Healthcare by *Modern Healthcare* and one of the Best Places to Work in Baltimore by the *Baltimore Business Journal* and the *Baltimore Sun*. Learn more at protenus.com and follow us on Twitter @Protenus.

About DataBreaches.net

DataBreaches.net is a website devoted to reporting on data security breaches, their impact, and legislative developments relevant to protecting consumer and patient information. In addition to providing news aggregation from global sources, the site also features original investigative reporting and commentary by the site's owner, a healthcare professional and privacy advocate who writes pseudonymously as "Dissent."

Methodology

The purpose of this section is to explain decisions that were used to guide the analyses. Incidents included in the analyses for this report were compiled for Protenus by DataBreaches.net, with additional research and analyses provided by Protenus.

Sources

Incidents were included in our analyses if they involved health-related or medical information about U.S. residents or citizens and if the incident was first disclosed between January 1, 2021 and December 31, 2021. The collection of reports stopped on January 4, 2021. Because we have used an earlier cutoff date for collecting December reports than in previous years, our numbers for December are somewhat lower than they would be otherwise.

As in our past reports, not all entities included in our analyses are medical entities or HIPAA-covered entities. While our analyses include incidents that appear on the U.S. Department of Health & Human Services public breach list, other sources included:

Incidents reported to state regulators when such reports could be found online. For 2021, we did not have reports from the Maryland Attorney General's Office for the full year as they had not updated their site past May at the time we stopped data collection for the year. Based on previous years and months, we estimate that there might have been another 50 or more reports if we had had all of their data; and Incidents based on investigative journalism by DataBreaches.net that may not have been reported to federal or state regulators. These incidents include verified data leaks discovered by researchers as well as confirmed breaches by threat actors that were not or had not yet been disclosed to regulators.

Even though the one source for a number of incident reports was not updated after May, and in the last few months of the year, threat actors added victims' names to their dark web leak sites but proof of hack/exfiltration has not been disclosed by either party, our analysis identified more new incidents and more breached records than in 2020.

Coding of Incidents

The Breach Barometer uses a coding system different than that used by HHS in its breach tool:

HHS codes some incidents as "unauthorized access/disclosure." That category could include incidents of insider wrongdoing/snooping, but it could also include external threat actors or just misconfigured databases that expose information. Protenus's coding system distinguishes insider/employee events from external actor incidents and includes misconfiguration-based exposures or leaks as insider error.

HHS' "hacking/IT incident" category could mean an external hack, but it could also mean any other type of IT incident that might not involve an external threat actor. The Breach Barometer uses the "hack" category for external threat actors, and where known, we provide additional data on whether the attack involved email (as in phishing) or extortion (as in ransomware) demands. If neither category appeared appropriate or we had insufficient information, the incident was tabulated under a "general hacking" subcategory. In many cases, incidents reported as hacking incidents may have been ransomware incidents, but we could not code them as such because the entity never confirmed or acknowledged it. Because most entities generally do not provide a lot of details about the attacks, readers who tend to be conservative in interpreting analyses may feel safer just using the total number for the overall hacking category.

As we have done in the past, in the event of a breach involving a vendor or Business Associate, we counted that as (only) one breach, even if there are dozens of covered entities reporting it to patients or regulators. Thus, what HHS may count as 7 reports, and what other analyses may report as 7 incidents, the Breach Barometer counts as 7 reports but only 1 new incident.

In 2021, there were some big breaches involving attacks on BAs or vendors, but the Breach Barometer tends to underestimate the true scope of such incidents because:

Not all affected entities name or even note a BA or vendor in their breach reports to HHS or the public; and When some business associates report incidents to regulators, they may not specify how many covered entities or clients are included in their report, which also leaves us wondering whether their reported numbers include numbers reported directly by some of their clients.

"Insider Error" or "Insider Wrongdoing?"

Occasionally, we did not have enough information to determine whether a breach involving employees was really accidental or not. When protected health information (PHI) is disposed of improperly, it may be an accident involving a crew or contractor, or it may be that someone got lazy and knew what they were doing was wrong. Thus, the "insider-wrongdoing" category includes snooping, criminal behavior incidents (such as ID theft involving patient data), and also other willful misbehaviors that result in HIPAA violations.

Who Reports Incidents?

The HHS public breach tool contains a field that indicates what type of covered entity reported the incident in their records: a provider, a business associate, a clearinghouse or a health insurance plan. That reporting system is confusing, as in many cases, providers report incidents that occurred at a BA, but the entry does not indicate that any BA was involved. The Breach Barometer does include some statistics on who discloses incidents or reports them first, but because not all incidents in our analyses involve HIPAA, our coding system includes reports by businesses, the media, or other miscellaneous entities. In 2021, we continued to tabulate reporting data, but note that it is not as informative as one might wish, as there are many cases where the first disclosure was not by the breached entity or a BA, but by a researcher, the media or even ransomware threat actors. "Who reported the breach to HHS or regulators?" and "Who was responsible for security of the data that were breached?" are not the same questions as, "How did we all first find out about the breach?"

Keeping the above, in mind, the Breach Barometer findings generally underestimates the number of health plans involved. Many businesses have self-insured health plans, but when they have a breach, there may be no report publicly available on the HHS breach tool for breaches impacting more than 500. In many cases, we code a business entity or educational organization entity as "miscellaneous" because they may issue a press release that mentions medical or health insurance information was involved in a data security incident without actually saying that the data came from a health plan or some other source.

Calculating Gap to Discovery and Gap to Reporting

How long did it take for breaches to be discovered, and how long did it take for breaches to get reported or disclosed publicly? The inclusion of numerous third-party incidents resulted in the decision that for purposes of determining time intervals for "date of the breach to date of discovery" and "date of discovery to date of the public report," we would define the "discovery date" as the date that the third party first discovered the breach and not the date that they first informed the covered entity about it (even though covered entities use the date they were first informed as to the date of discovery in starting a 60-day clock to notify). As in past years, if we only knew the month or year the breach first occurred, we used the first day of the month or year in our calculations.

In calculating time intervals between the date of the breach and the date of the public report, we defined the date of the public report as the date that the entity reported the incident to HHS or a regulator, sent letters to affected patients or members, or issued a press release. We note that in many cases, the entity's public disclosure might be months after threat actors, researchers or the media actually first disclosed breaches. It may also be months after patients' protected health information may have been dumped on the dark web by threat actors whose ransom demands were ignored or refused.

In 2021, as in 2020, we noted that many entities treated the date that they first discovered PHI was involved in an incident as their "date of discovery" to start the 60-day notification clock. So if they discovered a breach of their system on January 5, but only first discovered PHI was involved on March 6, they treat March 6 as the date of discovery. Some entities went even further in misdefining the date of discovery by treating the date that they finished identifying everyone who needed to be notified as their "date of discovery." Neither definition is consistent with HIPAA or HITECH's definition of "discovery," but HHS has not taken any enforcement action on this issue as of the time of this report.

Largest New Incident of the Month

Although the largest new incident in any month is the most unstable statistic, we have included it in our report. For some months, however, we did not have even imprecise numbers for what were likely the largest new incidents of those months. Similarly, other large breaches involving BAs were often reported piecemeal over months, confusing any attempt to determine the largest new incident disclosed in a month.

State Data

For state frequency data, if a BA or vendor was responsible for the breach, we entered one report into the state frequency counter for the first entity that disclosed the breach, but we did not enter all of the covered entities' states that month or in subsequent months. Thus, the state frequency map is not a frequency map for all reports, but a frequency map of the first report of new incidents. A breach involving a BA got charged to the state where that BA is headquartered in cases where we knew the identity of the BA.

For Further Information on Methodology

Any inquiries about the data collection or analyses should be directed to marketing@protenus.com.

Disclaimer

This report is made available for educational purposes only and "as-is." Although we have tried to provide accurate information, as new information or details become available, any findings or opinions in this paper may change. Despite our diligent efforts, we remain convinced that the breaches we find out about publicly are only the tip of a large iceberg.