PROTENUS®

2021 BREACH BAROMETER®

Hacking incidents jump 42% while insider incidents skyrocket during COVID-19 pandemic

Protenus, Inc. in collaboration with DataBreaches.net

As healthcare battles COVID-19, **hacking incidents jump 42%.**

CONTENTS

01 INTRODUCTION

Effects of COVID-19 4

02 OVERVIEW OF 2020 FINDINGS

758 Health Data Breaches 5

03 INSIDER INCIDENTS INCREASED

After Four-Year Decline 8

04 HACKING INCIDENTS ON THE RISE

Ransomware Increases 11

05 BUSINESS ASSOCIATE INCIDENTS

24M Breached Records 15

06 REPORTING BREACHES

Longer Discovery 17

07 STATE FREQUENCY

49 States Represented 19

08 CONCLUSION

Prioritize Health Data Security 20

09 ABOUT PROTENUS

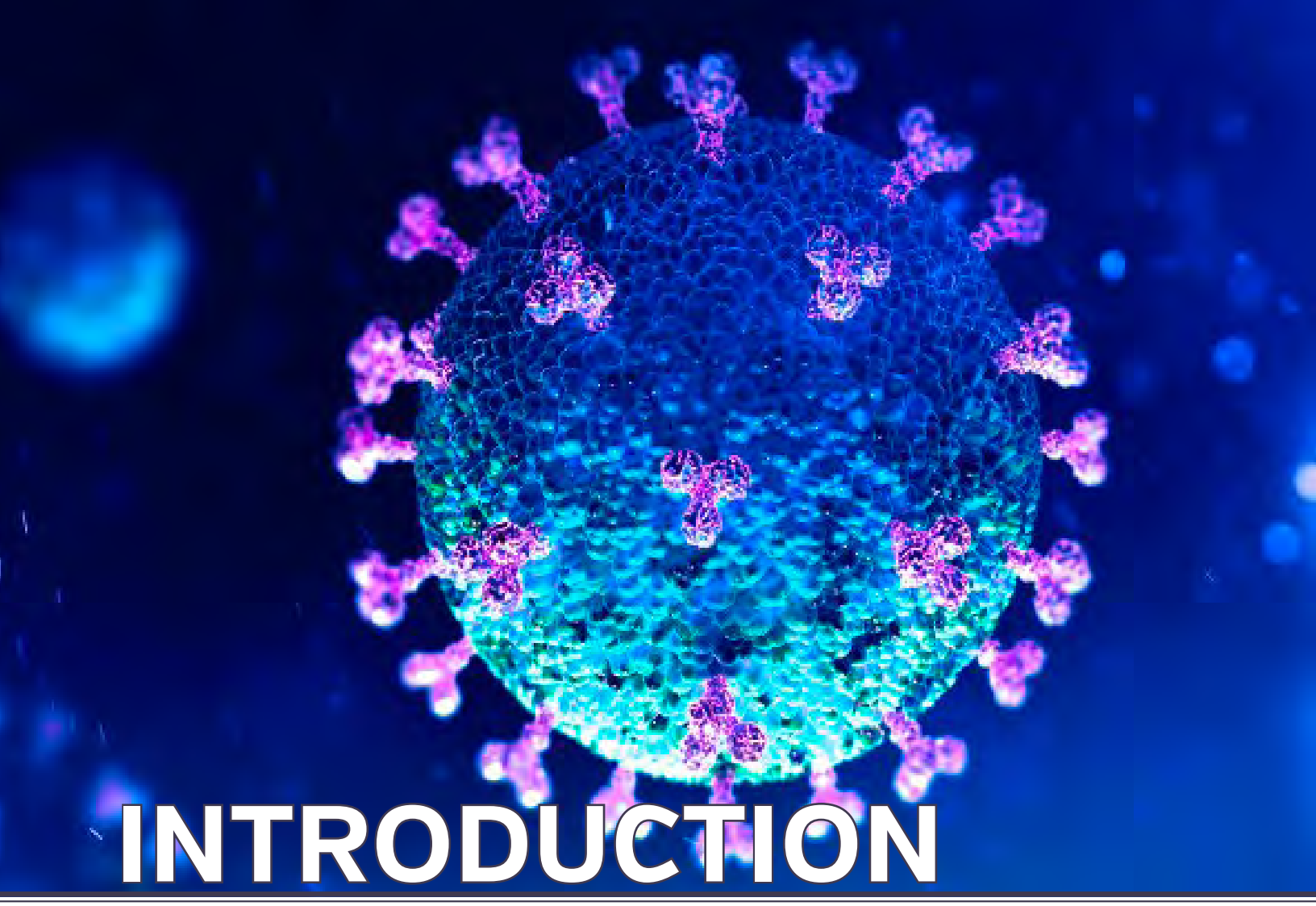
Learn More 21

10 ABOUT DATABREACHES.NET

Learn More 21

11 METHODOLOGY

Our Sources And Data 22



INTRODUCTION

Effects of COVID-19

In 2020, healthcare experienced unprecedented challenges as it grappled to get a handle on the varying components and associated effects of the COVID-19 pandemic. One ramification was the increase in breaches to patient data. The pandemic has unraveled progress the industry has made over the last several years and increased associated risk. Hackers have also taken advantage of a crippled system, with public reports of hacking jumping 42% from 2019. In October, the Cybersecurity and Infrastructure Security Agency, the FBI, and the U.S. Department of Health and Human Services (HHS) warned of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." Sadly, under-resourced and overrun hospitals continued to be a target for bad actors throughout 2020.

This retrospective report examines 2020 health data breaches with an eye toward lessons learned and a way forward for protecting patient privacy.

Overview of 2020 Findings

Our analysis is based on 758 health data breaches reported to HHS, the media, or some other source during 2020 (Figure 1). As in years past, we do not have detailed statistics for every incident in 2020, but in those 609 incidents for which we do have data, 40,735,428 patients were impacted. From 2019 to 2020, we saw an increase of more than 30% in the number of breaches reported— 572 in 2019 compared to 758 in 2020 — while the number of patient records affected was slightly lower year over year (Figure 2). It's important to know we won't fully understand the total volume of impacted patient records until investigations have been completed; we expect the true impact to be much higher.

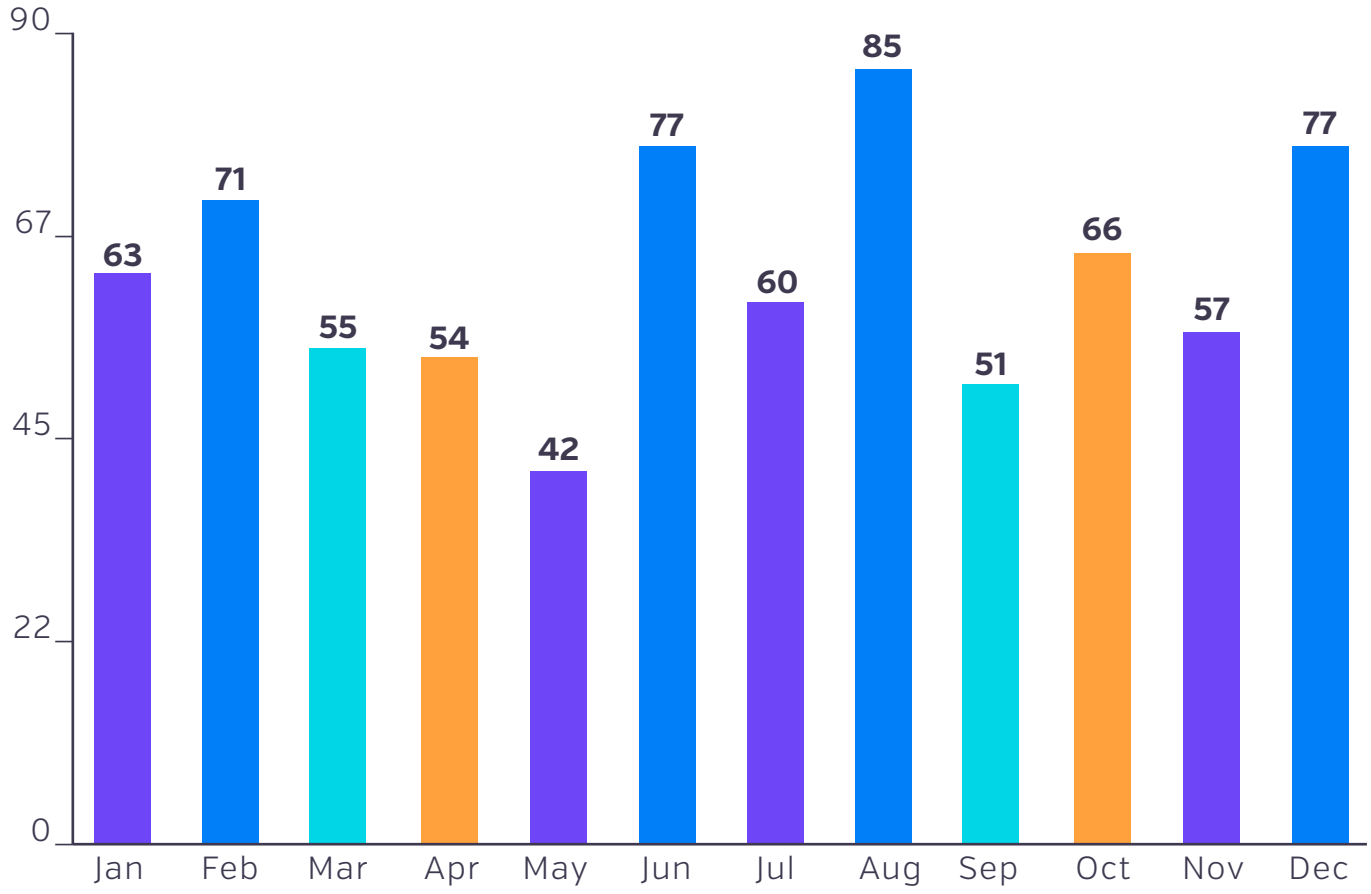


Figure 1. Total disclosed incidents, 2020 health data breaches

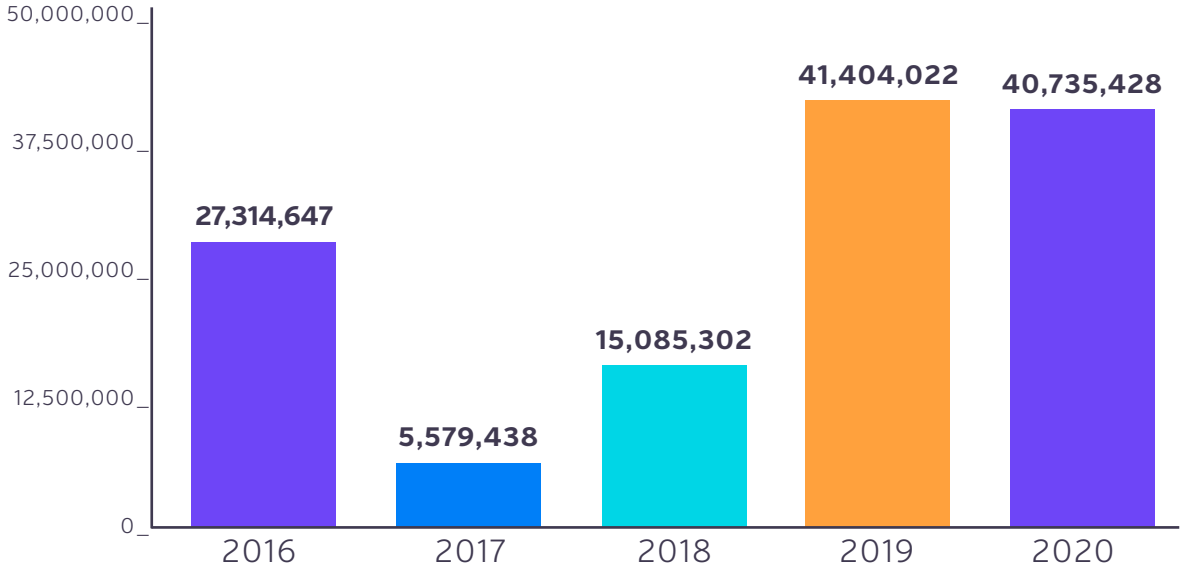


Figure 2. Total breached patient records, 2016-2020 health data breaches

Despite the continuing adoption of and advances in healthcare compliance analytics, the healthcare industry continues to grapple with data breaches. Since the Breach Barometer began in 2016, there has been an increase in the number of reported health data breaches every year (Figure 3). This trend has only been made worse by the resource-strained environments hospitals are operating under during the pandemic. Hospitals across the country are faced with increased costs in treating COVID-19 patients while having to eliminate the elective procedures necessary for financial stability. Compliance teams are also being moved away from their day-to-day responsibilities to help in other areas of patient care. However, the adoption of compliance analytics can ensure patient privacy and reduce costly risk across the organization.

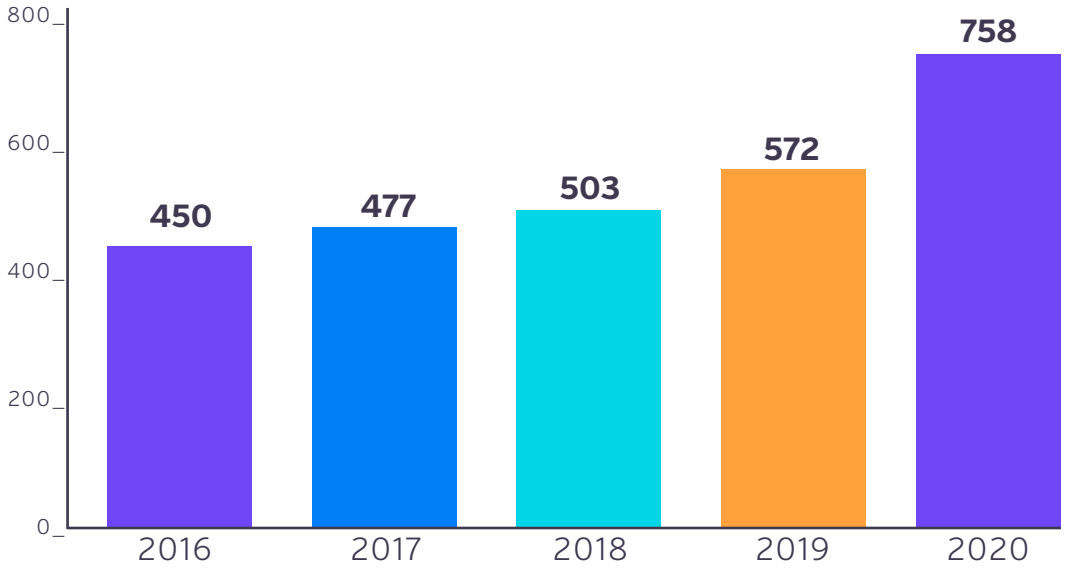


Figure 3. Total disclosed incidents, 2016 - 2020 health data breaches

2020 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
January	Business Associate	Insider-Error	700,000
February	Business Associate	Theft	654,362
March	Provider	Hacking	298,532
April	Provider	Hacking	112,211
May	Business Associate	Uncategorized	554,876
June	Health Plan	Hacking	1,650,600
July	Provider	Hacking	129,571
August	Business Associate	Insider-Error	3,100,000
September	**Business Associate**	**Hacking**	**3,320,726**
October	Business Associate	Hacking	829,454
November	Provider	Hacking	295,617
December	Business Associate	Hacking	1,290,670

Figure 4. Largest incidents, 2020 health data breaches

The Single Largest Breach

The single largest breach reported in 2020 (Figure 4) was the result of a hacking incident involving ransomware. The incident involved a large Catholic health system and its philanthropic data vendor, Blackbaud. In July 2020, Blackbaud notified the organization and other customers that they had fallen victim to a ransomware attack. The hackers gained access to the health system's donor database and were able to partially remove donor information that included date of birth, inpatient/outpatient status, contact information, and other sensitive patient information. The health system, under the guidance of Blackbaud's cybersecurity team and law enforcement, paid the ransom to ensure the hackers destroyed the information they had stolen and regain system functionality. This hacking incident affected 3,320,726 patient records. The Blackbaud ransomware attack affected several other organizations; this one is specifically noted because of the sheer amount of patient records affected from a single organization.

Insider incidents increase after four-year decline, affecting 8 million patient records

After a four-year decline in insider-related incidents, the healthcare industry saw an increase this past year (Figure 5). Since the start of the pandemic in March 2020, healthcare organizations have had increased concern that employees would violate patient privacy by snooping on colleagues suspected of having COVID-19 to gauge their own possible exposure to the virus. Even if the snooping isn't done for nefarious reasons, it still violates the patient's privacy and HIPAA regulations. It's also alarming that in 2020, the number of patient records breached by insiders more than doubled. As Figure 6 shows, the number of patient records affected by insider-related incidents drastically increased when comparing 2019 to 2020 data.

Insiders continue to pose significant risk to patient trust and can be costly for affected institutions. A New York-based medical center is among the many organizations affected by a similar kind of scandal in recent months. It began notifying patients in January that an employee, who has since been fired, illegally accessed electronic health records and viewed clinical information, including test results and diagnoses. Though the motive for snooping wasn't disclosed, the incident occurred from June to November 2020, as COVID-19 cases were surging.

Insiders were responsible for 20% of the total number of breaches in 2020, which is a slight increase from the proportion in 2019 (19% of total incidents). There was information for 111 of those incidents, affecting 8,505,742 patient records (21% of total affected patient records).

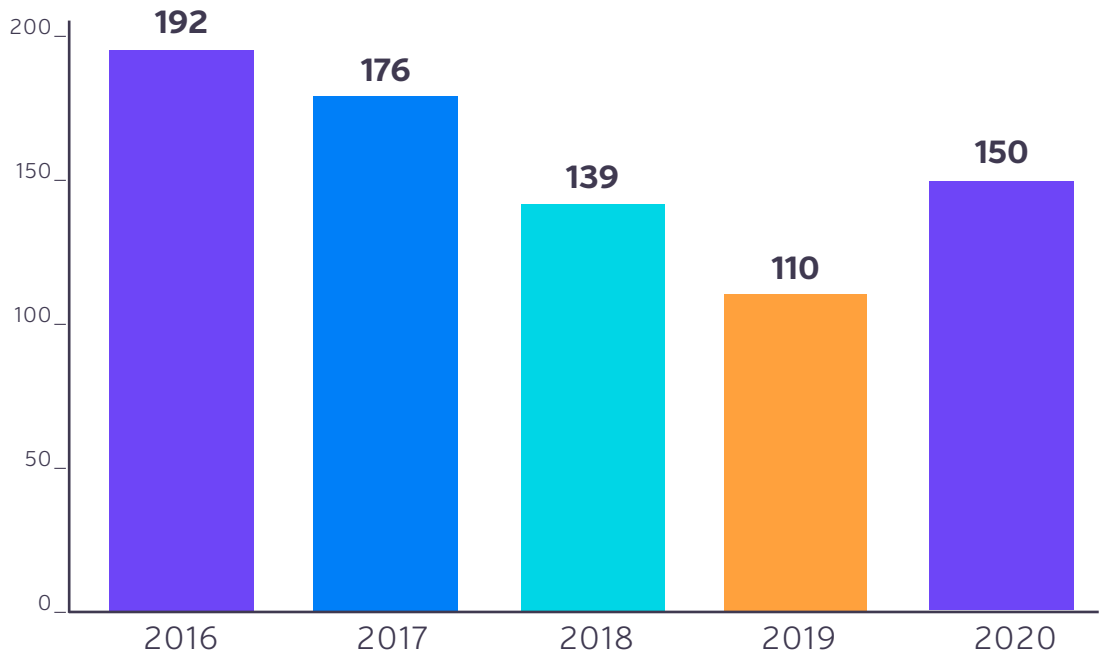


Figure 5. Total Insider-related incidents, 2016 - 2020 health data breaches

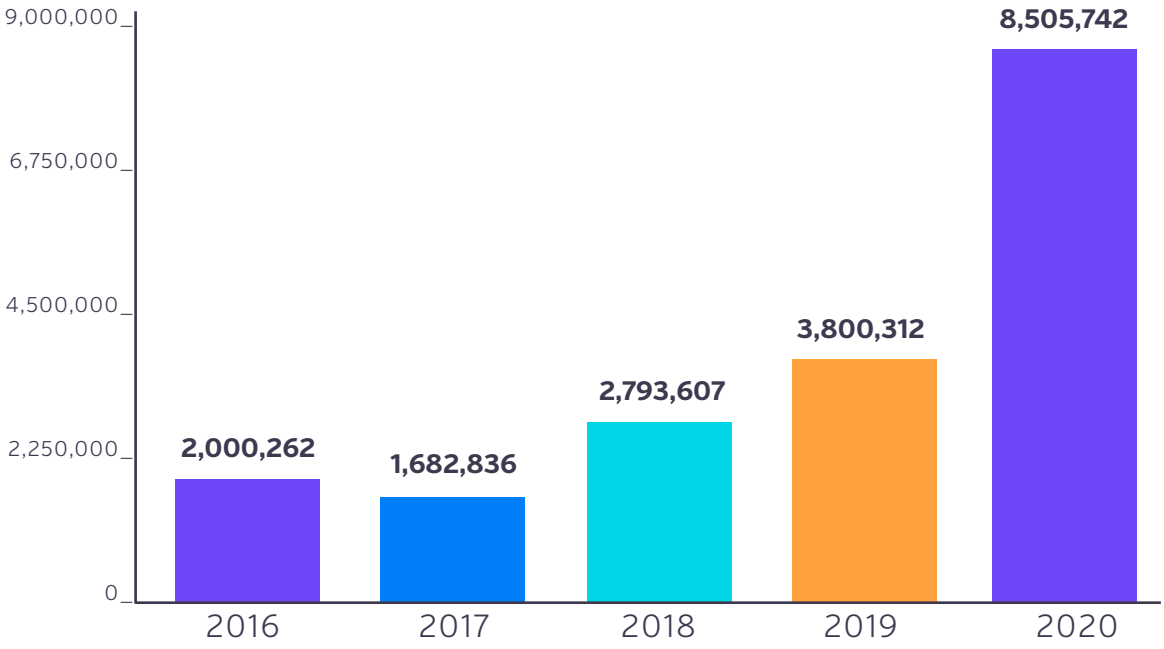


Figure 6. Number of breached patient records by insiders, 2016 - 2020 health data breaches

For the purpose of our analyses, we characterized insider incidents as either insider-error (I-E) or insider-wrongdoing (I-W). The former includes accidents and anything without malicious intent that could be considered "human error." Insider-wrongdoing includes employee theft of information, snooping in patient files, and other cases where employees appeared to have knowingly violated the law.

There were 96 incidents that involved insider-error in 2020, and we have data for 74 of them. In contrast, 45 incidents involved insider-wrongdoing, and we have information for 30 of these incidents. It is important to note that there are nine incidents for which there was not enough information to classify them as either insider-wrongdoing or insider-error. Insider-error affected 7,673,363 patient records and insider-wrongdoing affected 241,128 records.

While there were substantially fewer patient records breached by insider-wrongdoing, they are often more dangerous because employees with legitimate access to patient information can abuse their access with malicious intent, often undetected. In one case from 2020, a healthcare organization fired several employees for snooping on the record of a shooting suspect who died at the hospital. In another case, a Chicago-based hospital reported that an employee snooped on 4,800 patient records without a work-related reason. This employee inappropriately accessed these records from November 2018 to February 2020. Upon discovery, the employee was terminated and the organization took necessary steps to retrain employees on appropriate versus inappropriate access to patient information.

Noncompliance is critically important to identify and prevent, especially when organizations are struggling financially. Compliance incidents are costly because of all that goes into reconciling them. On top of paying penalties, health systems must do damage control. Fielding questions from the media and patients, fighting legal battles, and taking other reactive measures consume precious time and resources. Noncompliance may also cost an organization its reputation; a patient notified of a data breach may think twice about returning to the organization that let it happen. Such a scenario would be particularly detrimental mid-pandemic, when hospitals need revenue — and patients need no further reason to delay care.

Hacking incidents increase for fifth straight year

The healthcare industry experienced yet another increase in hacking incidents in 2020, as hackers took advantage of pandemic-related hardship. As Figure 7 illustrates, the increase is consistent with an alarming year-over-year trend dating back to 2016. Figure 8 illustrates that hacking incidents were relatively constant throughout the year, with a total of 470 incidents in 2020, comprising 62% of all 2020 breaches (Figure 9). For 277 of those incidents, we have data on how many patient records were exposed. These incidents combined affected 31,080,823 patient records (Figure 10). For comparison, in 2019, there were 330 hacking incidents, which affected 36,911,960 patient records (Figure 11).

It appears that ransomware incidents in particular are on the rise. For the second year, there have been public reports of hackers exploiting organizations and patients alike. One new trend that has emerged is ransomware threat actors naming victims who do not pay the ransom demands and threatening to publicly dump the data if they refuse to pay. To make matters worse, ransomware attacks more than doubled since 2019. Ryuk ransomware hit six hospitals across the country in October 2020, while the government issued a warning with a list of 400 targeted organizations. Affected hospitals ended up having to replace several thousand computers and reported IT outages due to the attack. As previously mentioned, Blackbaud was hit with a security breach that affected more than 46 hospitals and health systems. A separate incident forced the affected healthcare organization to revert back to paper records for several days while the systems were down. These types of attacks serve as a wake-up call for organizations across the country to adopt healthcare compliance analytics to better protect patient information and prevent future care disruptions.

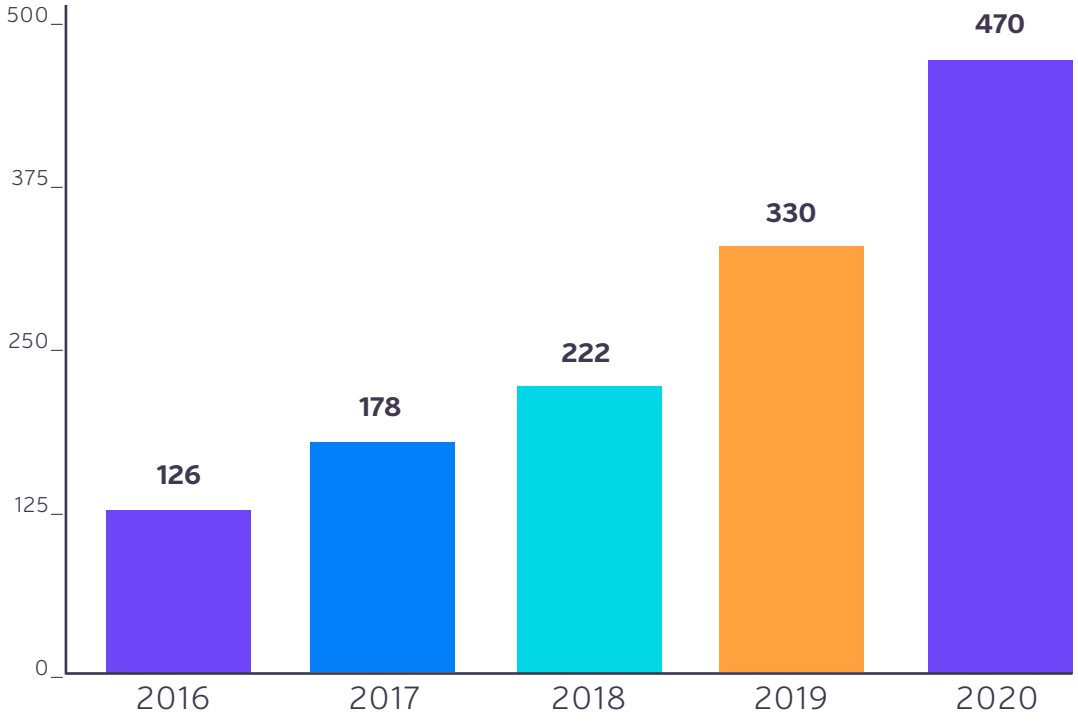


Figure 7. Total hacking incidents, 2016 - 2020 health data breaches

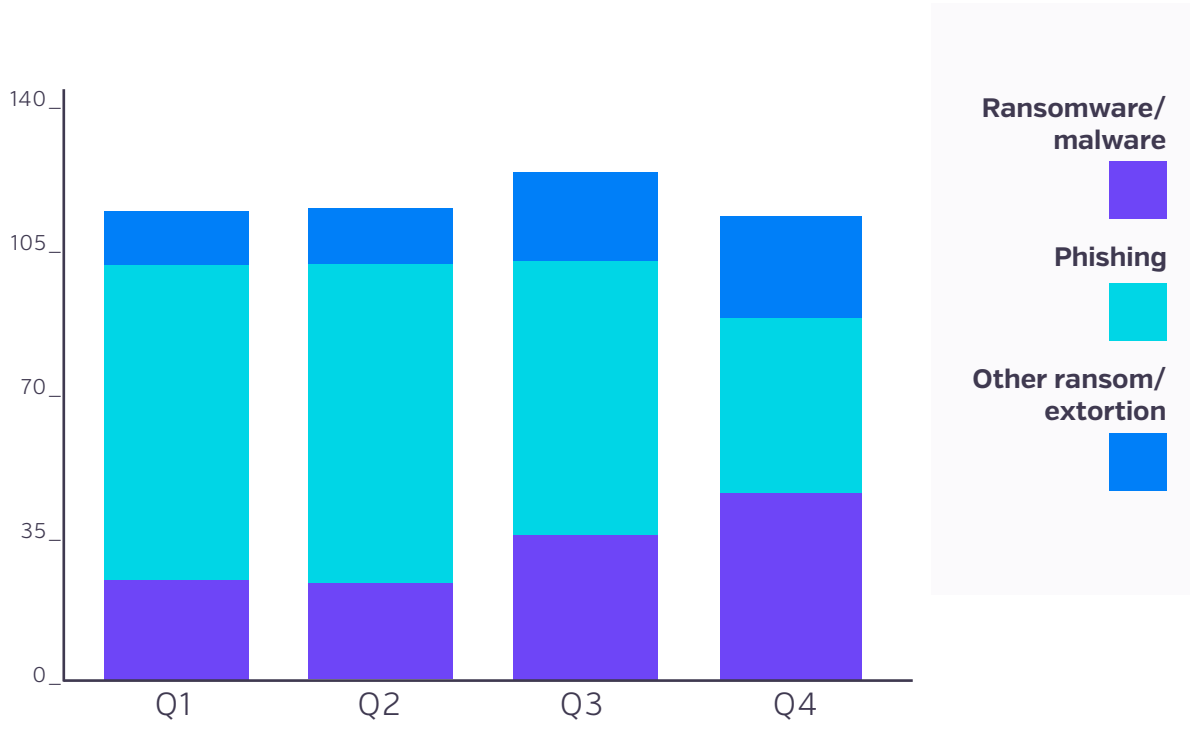


Figure 8. Total hacking incidents, 2020 health data breaches

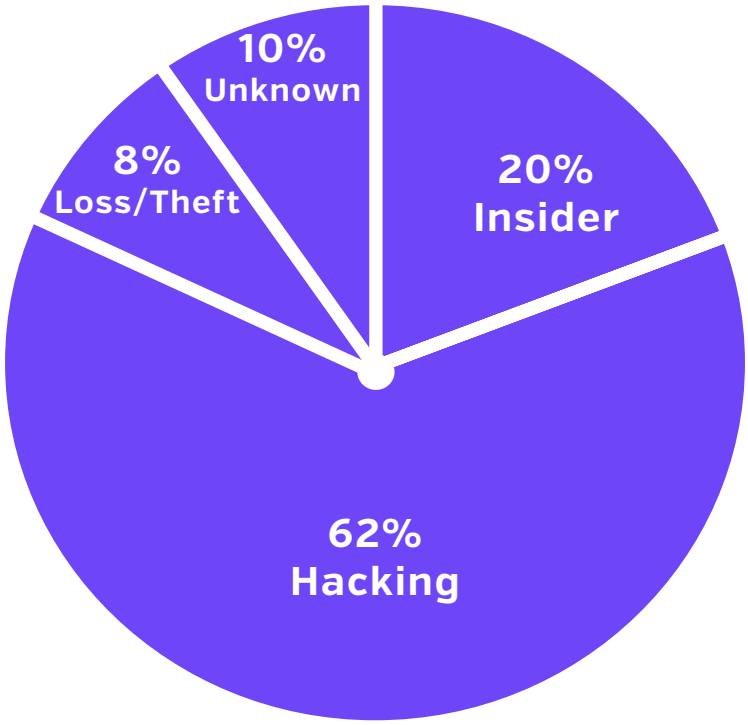


Figure 9. Type of incidents, 2020 health data breaches

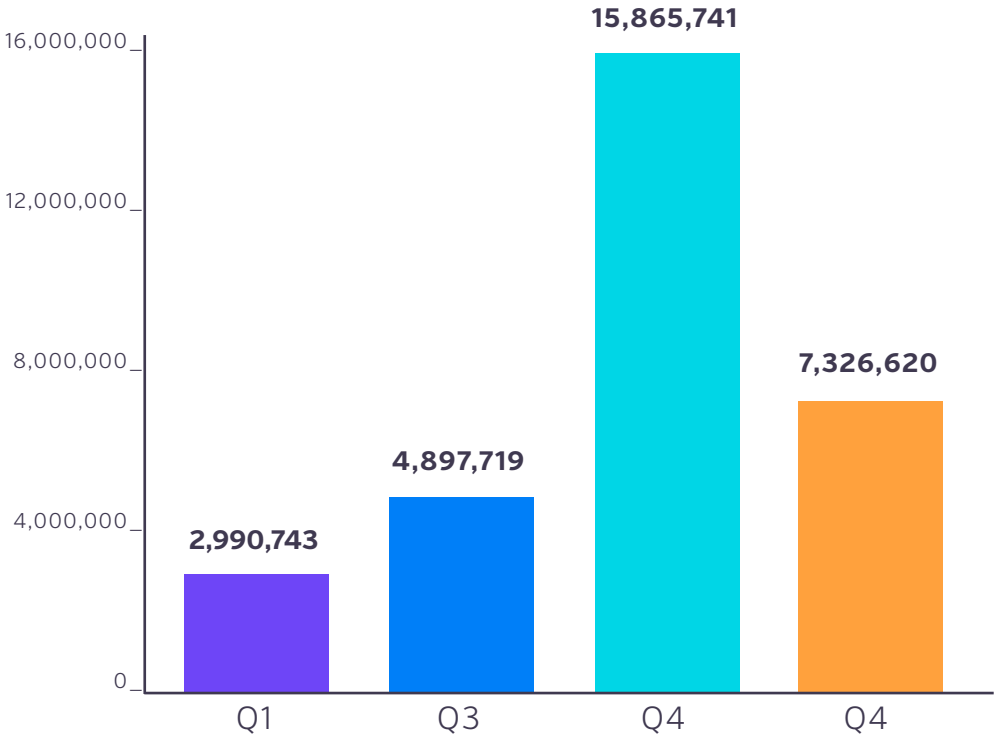


Figure 10. Patient records breached by hacking, 2020 health data breaches

For healthcare organizations to get ahead of these hackers, risk assessment and employee training and education are crucial. Organizations need to ensure they are testing to make sure the appropriate security measures are working as intended and that backups are separated from the main network, so an attack cannot spread to the backups as well.

Employee training is also critical in preventing phishing attacks. Healthcare compliance teams need to ensure their employees know how to spot a phishing email and what to do when they receive one.

Besides hacking and insider incidents, there were also 48 breaches due to theft. We have data for 43 incidents, which affected 834,077 records. Sixteen incidents involved missing or lost records, potentially exposing the information of 59,159 patients.

Finally, there were 74 incidents that could not be categorized due to insufficient information. We have numbers for 66 such incidents, affecting 255,627 records.

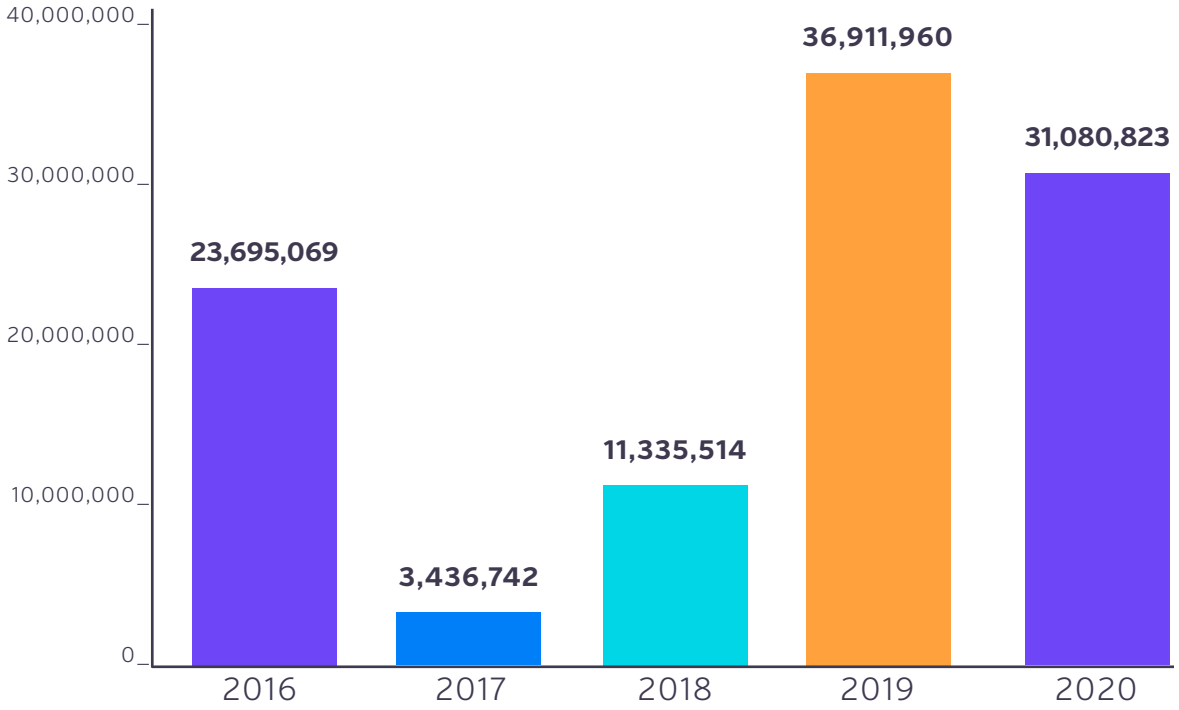


Figure 11. Patient records breached by hacking, 2016 - 2020 health data breaches

Business Associates responsible for 24M breached records

Of the 758 reported incidents in 2020, 492 involved healthcare providers (65% of all reporting entities), 75 involved health plans (10%), 94 involved a business associate (12%), and 97 (13%) involved some other type of entity (Figure 12).

For the purpose of this report, business associates (BA) are defined as third-party vendors contracted by health systems to conduct business or provide services on behalf of the healthcare organization.

For the BA incidents for which we had numbers, 24,345,220 patient records were affected. Figure 13 shows that hacking incidents involved the largest proportion of BAs (55% of BA-involvement), followed by insider-error incidents. Even with the large number of affected patient records from BA-involved incidents, it should be noted that there could be even more incidents involving third parties, but there was not always enough information to make that determination.

Finally, even though most healthcare organizations have already switched over to electronic health records, 101 incidents involved paper records (13% of total incidents, Figure 14). These incidents affected 1,048,610 patient records. It is possible that there are more breaches involving paper records, but again, some reports lacked sufficient detail to make that determination.

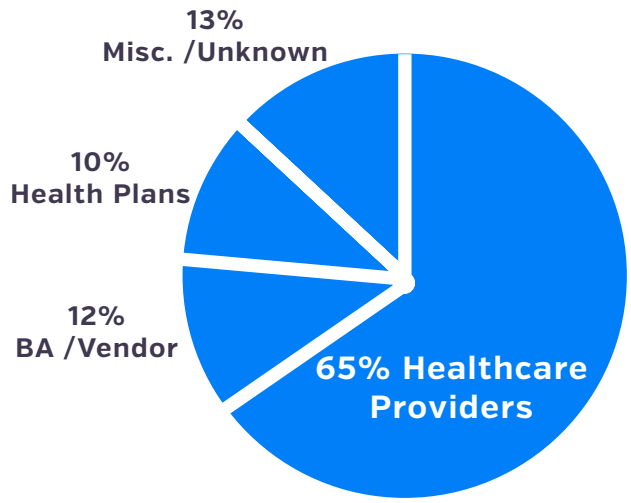


Figure 12. Types of entities reporting, 2020 health data breaches

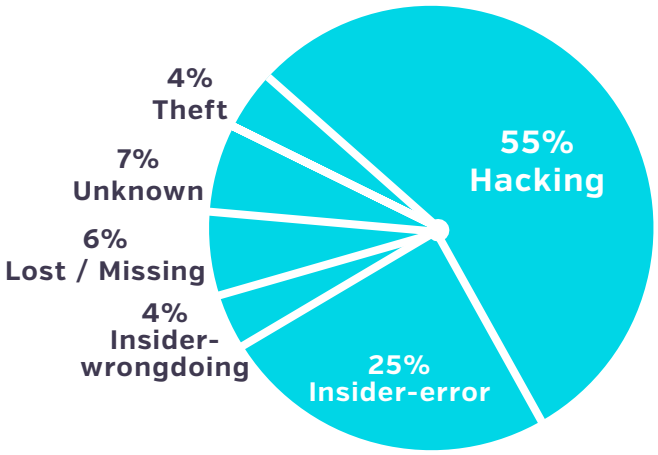


Figure 13. BA/third-party involvement, 2020 health data breaches

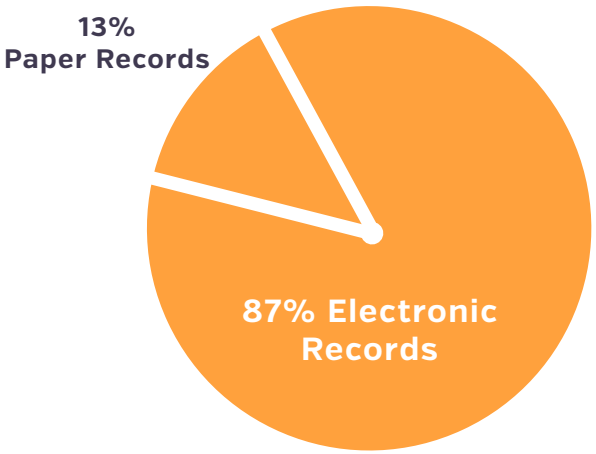


Figure 14. Paper vs. electronic records, 2020 health data breaches

Organizations are taking longer to report breaches

As illustrated in Figure 15, it took an average of 187 days for a healthcare organization to discover that it had suffered a breach in 2020. This represents an improvement from 2019, when it took an average of 224 days for breach detection. The median discovery time in 2020 was just 15 days. It's important to note, however, that there were a wide variety of time frames for discovery, with the shortest discovery time being one day and the longest being several years.

Of the 339 health data breaches for which we have data, it took an average of 85 days for organizations to report a breach to HHS, the media, or other sources after it was discovered (Figure 16). The average increased slightly when compared to 2019 data with an average of 80 days for reporting. The median disclosure time was 60 days, which meets the HHS required 60-day reporting window.

It's important to note that the dataset for this analysis varies greatly from month to month, and data on time to disclosure wasn't available for every incident that occurred in 2020. As a result, the smaller data set may not provide a complete picture of reporting times throughout the year.

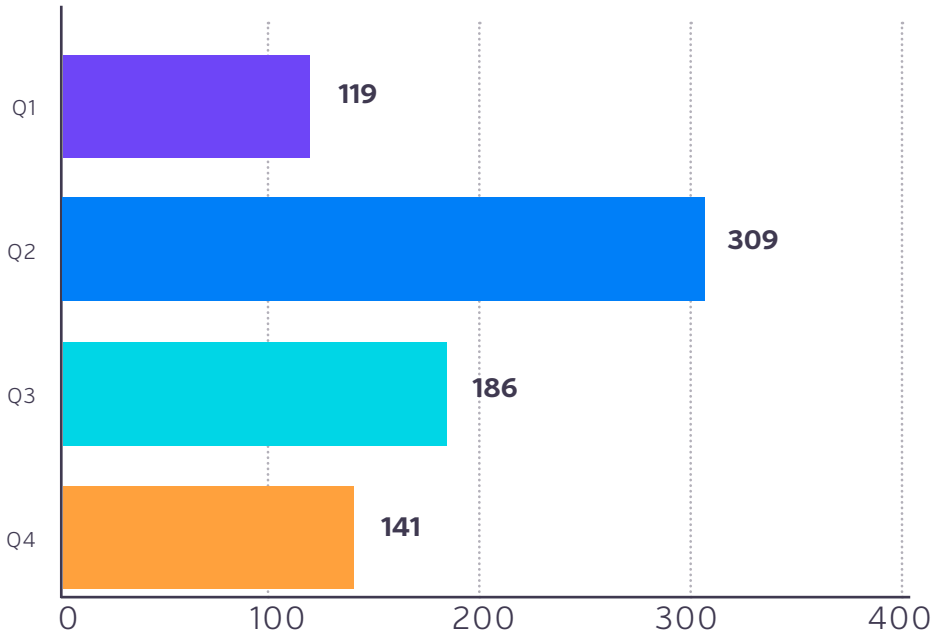


Figure 15. Average number of days from breach to discovery, 2020 health data breaches

While hacking incidents may be discovered more quickly than insider incidents, they also tend to have longer gaps between the discovery of the breach and reporting it. This may be due to ransomware attacks making it more difficult to determine what may have been accessed or exfiltrated, making it harder to identify who to notify.

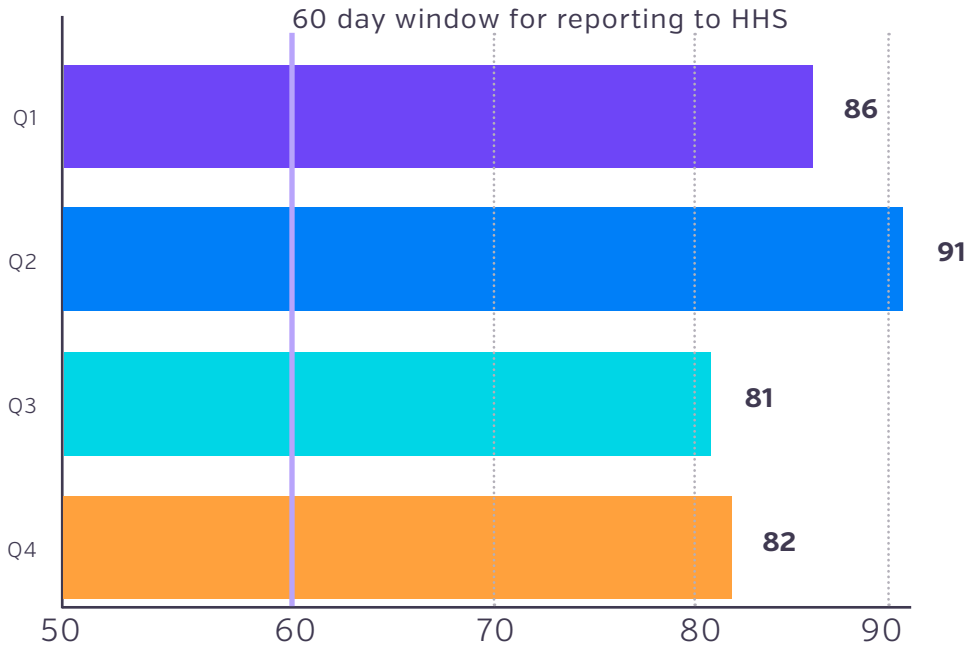


Figure 16. Average number of days from discovery to reporting to HHS, 2020 health data breaches

State Frequency

Forty-nine states (98%) and Puerto Rico are represented in the 758 incidents for which we had location data. Only one state did not have any reported breaches: Wyoming. California had the most reported incidents with 75, followed by Texas with 59. Please note that numbers for some states are inflated because this analysis uses the state where the BA/vendor is located, not where the healthcare organization is located.

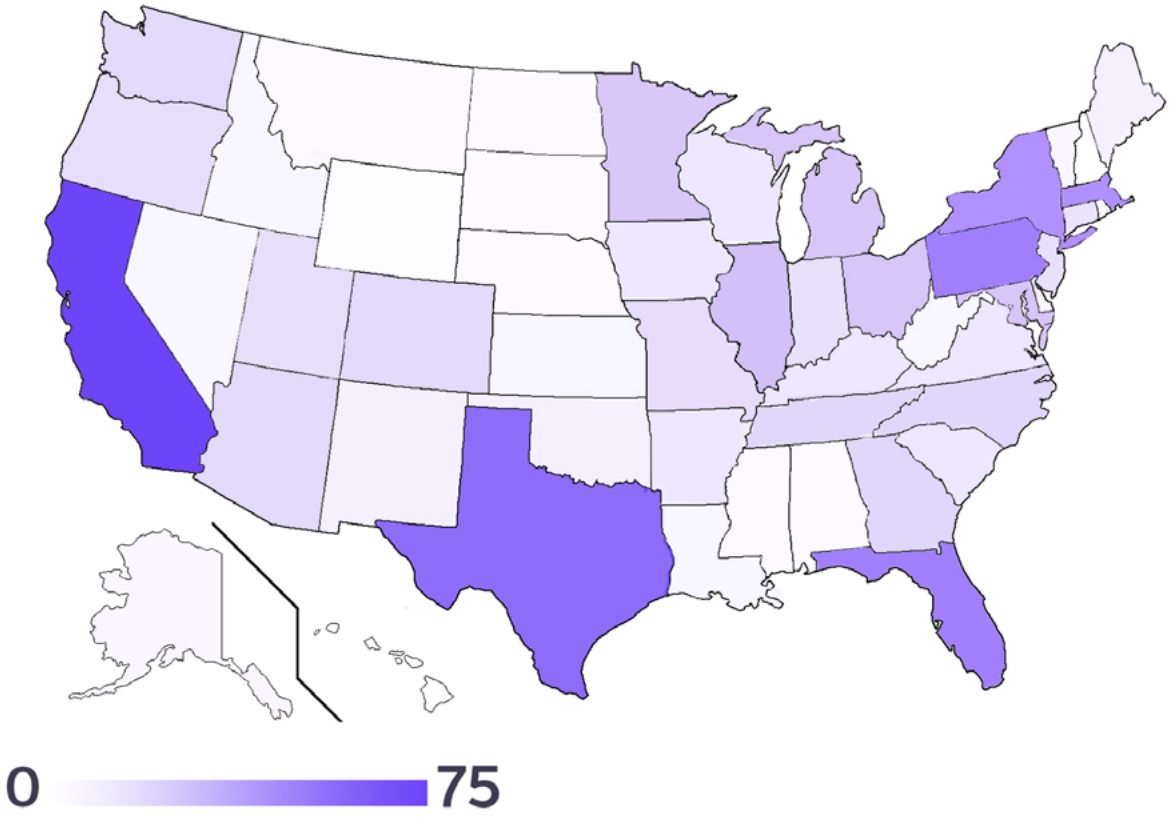


Figure 17. Number of incidents by state, 2020 health data breaches

Conclusion

The data has shown an increase in health data breaches year over year since 2016, but none have increased as much as we saw with the COVID-19 pandemic. The current climate has increased risk for health systems as a new trend emerged of at least two data breaches per day, a troubling sign of the continuing vulnerability of patient information, heightened by the pandemic. While the pandemic persists in 2021, the only way the industry will be able to reverse course will be by leveraging cost-effective strategies that quickly identify risky behavior without taking resources away from patient care. Healthcare organizations need to leverage technology that allows organizations to maintain compliance priorities in a resource-constrained environment. Hospitals can't afford the costs often associated with these incidents, as more than three dozen hospitals have filed bankruptcy over the last several months. Non-compliance is not an option.

2021 will remain difficult for healthcare organizations as they continue to struggle with COVID-19 hot spots and financial vulnerability. Overall, the industry is getting better at breach detection and prevention by leveraging technology like healthcare compliance analytics to reduce overall risk to their organizations. Even with this adoption of new technology, it remains vitally important to educate and train hospital employees on how to detect and not fall victim to phishing attacks. This will be imperative to getting ahead of the hacking incidents currently plaguing healthcare. Health data security will need to remain a top priority, gaining necessary insight into how data moves through each organization and when there are threats that need to be mitigated. Armed with the latest information and utilizing the latest advances in technology, the healthcare industry can gain visibility into patient data access, ultimately making institutions more secure and reducing risk across each organization.

About Protenus, Inc.

The Protenus healthcare compliance analytics platform uses 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 prevention, better protecting their data, their patients, and their institutions. In 2020, Protenus was named one of Forbes' Best Startup Employers, one of CBInsights Digital Health 150, and the 2020 KLAS Category Leader in Patient Privacy Monitoring. In 2019, Protenus was 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 analyses provided by Protenus.

SOURCES

Incidents were included in the 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, 2020, and December 31, 2020. Not all entities are medical or HIPAA-covered entities.

- Incidents reported to the U.S. Department of Health & Human Services (HHS) that appear on the agency's public breach tool
- Incidents reported to other federal or state regulators, e.g., SEC filings and state-mandated notification to states when such reports could be found online
- Publicly disclosed incidents involving organizations or entities that are not HIPAA-covered entities but where the incidents involved what would be considered protected health information elements under HIPAA; and
- Incidents based on investigative journalism by DataBreaches.net that may not have been reported to federal or state regulators, but were discovered by independent researchers and shared with DataBreaches.net for reporting, notification to entities, and investigation.

As in past years, incidents were included even if there was no confirmed data breach, i.e., potential breaches involving data exposure and ransomware locking up databases with patient data were included even if there was no evidence that data were accessed by threat actors or downloaded.

CODING OF INCIDENTS

As in the past, the Breach Barometer analyses use a coding system different than that used by HHS in its breach tool. HHS, for example, 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' coding system breaks out insider/employee events from external actor incidents, and includes misconfiguration-based exposures as insider errors. Similarly, HHS's category "Hacking/IT Incident'' 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 phishing, malware, or extortion demands.

BUSINESS ASSOCIATE INCIDENTS

When a breach involving a vendor or Business Associate was reported, (only) one new breach for the month tallied, even if there are dozens of covered entities reporting it to patients or regulators. Numbers reported by the covered entities were included in the analysis of the number of records breached, but not as separate incidents. In subsequent months, newly revealed numbers are included in breached records for the month but not counted as a new incident for the month.

WHO REPORTS INCIDENTS

HHS's public breach tool contains a field that indicates what type of covered entity reported the incident in their records – either a provider, a business associate, a clearinghouse, or a health insurance plan. But the agency's reporting system is confusing, as in many cases, providers report incidents that occurred at a business associate, but the entry does not indicate that any business associate was involved. Our report 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 2020, we continued to tabulate reporting data, but note that it is not as informative as one might wish and that it would be more helpful, perhaps, to have clearer measures and reporting to HHS and to states and federal agencies as to whether a third party was responsible for an incident.

CALCULATING GAP TO DISCOVERY AND GAP TO REPORTING

The inclusion of numerous third-party incidents resulted in the decision that for purposes of determining time intervals for "date of breach to date of discovery" and "date of discovery to date of 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. In calculating time intervals between date of breach and date of public report, we defined the date of public report as the date that the entity first reported the incident to HHS or a regulator, or the date that there was a media report or an announcement made to the public.

In many cases, we do not have exact dates, but only know the month or year the breach first occurred. In calculating the interval between the breach to discovery and between the breach and reporting:

- If data was only available for the month or year of the breach, the first day of the year or month was used for calculation purposes.
- The date a BA/vendor first discovered the breach was used as the discovery date and not the date the covered entity first learned of the breach.

"Date discovered" is defined as the date a covered entity first learned that protected health information had been compromised.

LARGEST INCIDENT OF THE MONTH

The largest incident of the month can sometimes be an unstable statistic as numbers were not available for what were likely the largest incidents of those months. Similarly, other large breaches involving BAs were often reported over several months, making it difficult to determine the largest new incident disclosed in a given month.

Whenever we were aware that an entity's report was part of a BA breach that affected multiple entities, we counted the incident as one incident. When additional reports came in from other affected entities over the next months, they were not counted as new incidents for those months, but their number of records were added to the number of records for those later months. Thus, for each month, the number of incidents should be understood as the number of newly disclosed incidents with all reports linked to one business associate treated as (only) one incident, although additional records might be disclosed and counted in subsequent months when they were first reported for additional affected entities.

STATE DATA

For state frequency data, if a BA or vendor was responsible for the breach, we assigned the breach to the state where the BA or vendor is headquartered or located, and did not count each covered entity impacted by the BA breach as part of our analysis. In cases where the third party's location could not be determined, the incident was assigned to the covered entity's state.

FOR FURTHER INFORMATION ON METHODOLOGY

Any inquiries about the data collection or analyses should be directed to kira@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, and any patterns we see in publicly disclosed breaches may not mirror what goes on beneath the surface.

PROTENUS®

2021 BREACH BAROMETER®

contact@protenus.com | protenus.com