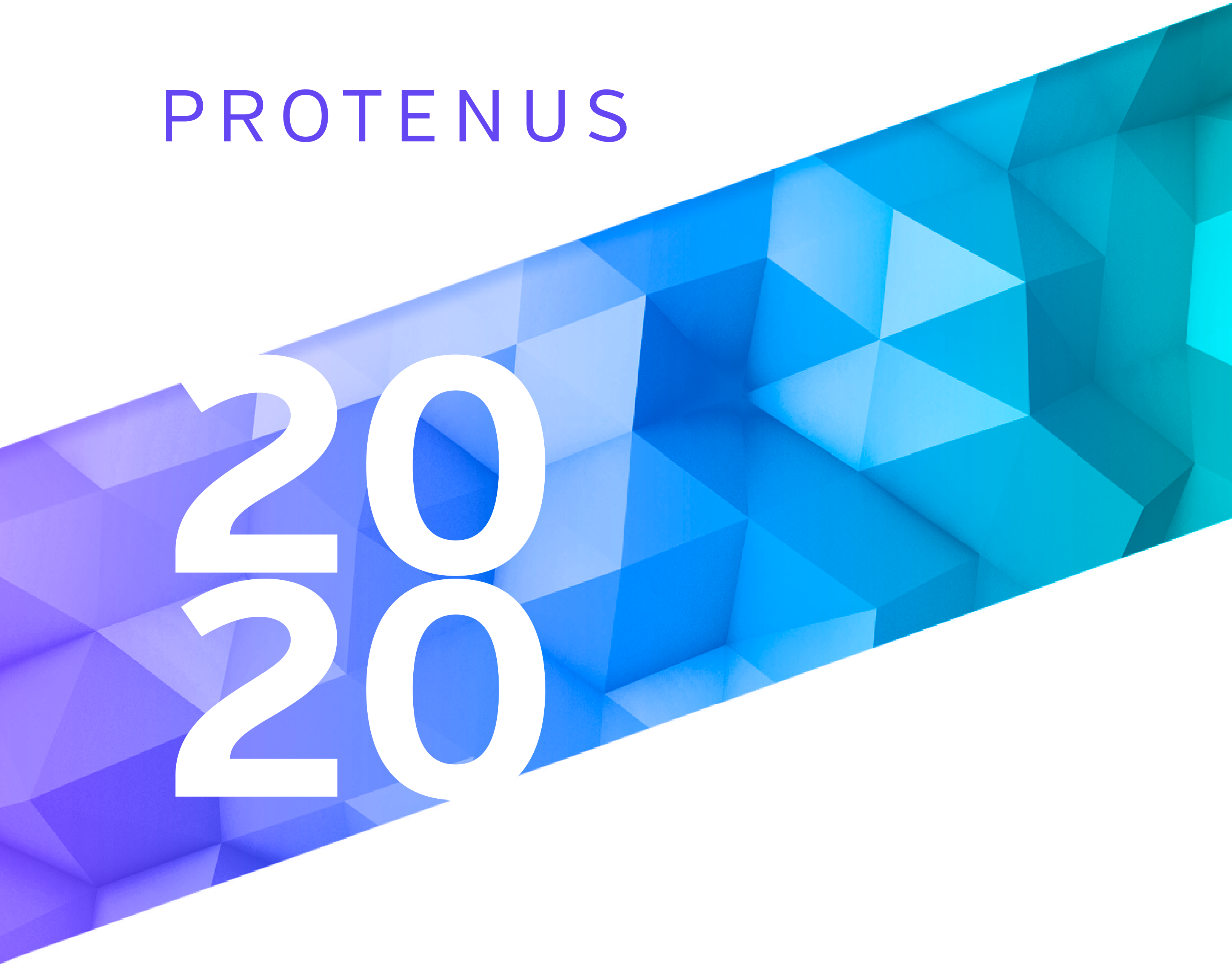
PROTENUS



2020

BREACH BAROMETER

41M+ patient records affected in 2019 as hacking incidents continue to escalate

As seen in: CBS THIS MORNING U.S.News & WORLD REPORT engadget CBS NEWS

With health data breaches on the rise since 2016, **healthcare needs to take action**.

CONTENTS

INTRODUCTION

Protecting Patient Privacy

In 2019, the healthcare industry continued to be plagued by data breaches involving sensitive patient information, with public reports of hacking jumping a staggering 48.6% from 2018. This staggering number of reported hacking incidents reminds us how vulnerable patient data remains. Unfortunately, patient information can still be easily accessed and obtained by healthcare insiders and external actors alike. Although the healthcare industry understands the importance of protecting patient data, the trend of at least one health data breach per day persists- and has increased since 2016.

This retrospective report examines 2019 health data breaches with an eye toward lessons learned and a way forward for protecting patient privacy.

Overview of 2019 Findings

Our analysis is based on 572 health data breaches reported to the U.S. Department of Health and Human Services (HHS), the media, or some other source during 2019 (Figure 1). As in years past, we do not have numbers for every incident in 2019, but for those 481 incidents for which we have data, 41,404,022 patients were impacted. This number is likely to be a huge underestimate, as two of the incidents for which there was no data affected 500 dental practices and clinics and could affect significant volumes of patient records. Comparing these numbers with those of last year, we saw an increase in the number of breaches reported (503 in 2018 compared to 572 in 2019), and a staggering increase in the number of affected patient records (Figure 2). In 2019, the total number of affected patient records almost tripled when compared to 2018 data (i.e., 15,085,302 affected patient records).

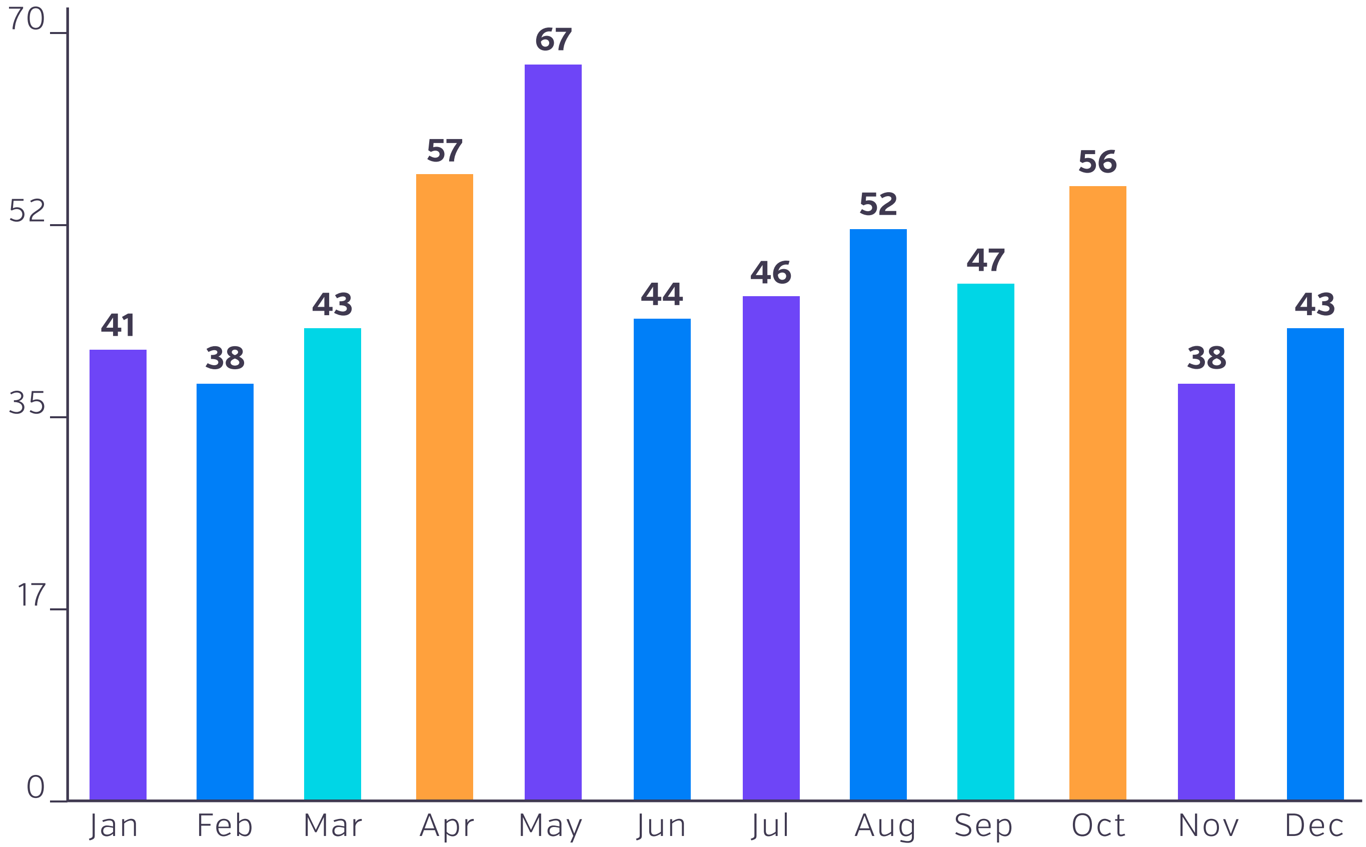


Figure 1. Total disclosed incidents, 2019 health data breaches

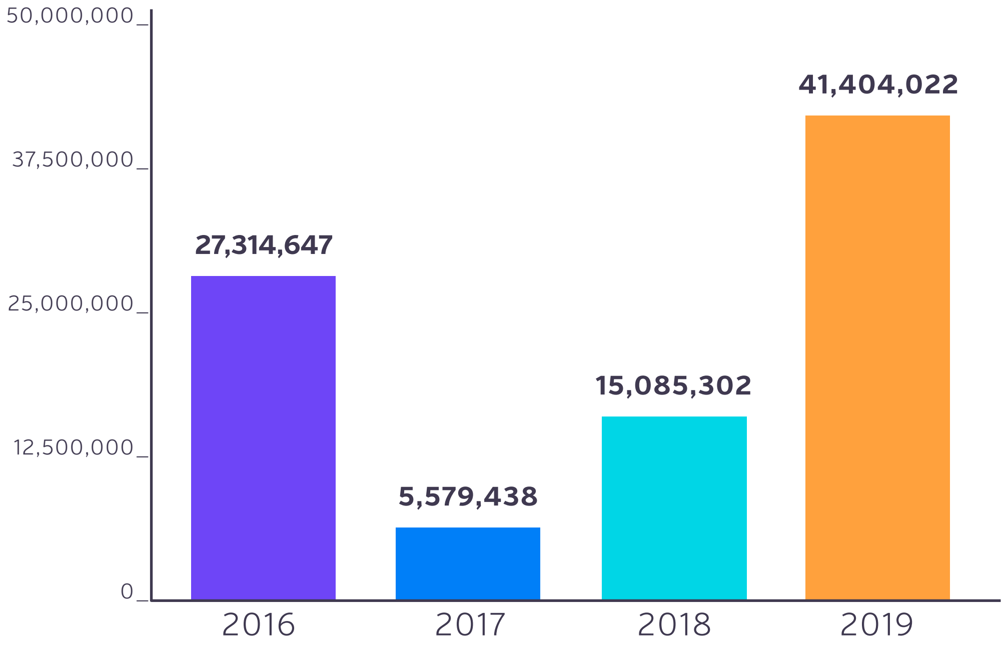


Figure 2. Total breached patient records, 2016-2019 health data breaches

Despite innovations in healthcare compliance analytics, the healthcare industry has continued to experience an increase in the number of reported health data breaches, year over year, since Protenus started compiling statistics in 2016 (Figure 3). This is an alarming trend which should change as more organizations deploy advanced patient privacy monitoring systems that can prevent future incidents.

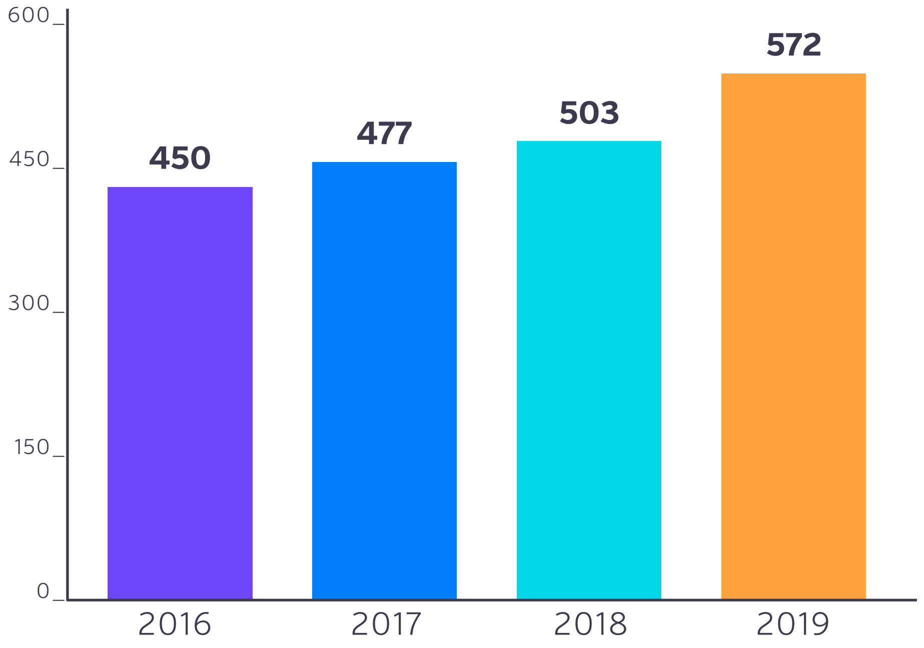


Figure 3. Total disclosed incidents, 2016 - 2019 health data breaches

2019 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
January	Business Associate	Hacking	111,529
February	Provider	Insider-error	973,024
March	Provider	Hacking	645,000
April	Business Associate	Insider-error	1,565,338
May	**Business Associate**	**Hacking**	**20,949,600**
June	Health Plan	Hacking	2,964,778
July	Provider	Hacking	2,234,500
August	Provider	Hacking	320,000
September	Provider	Hacking	528,188
October	Provider	Hacking	152,200
November	Provider	Hacking	125,000
December	Provider	Theft	114,466

Figure 4. Largest incidents, 2019 health data breaches

The Single Largest Breach

The single largest breach reported in 2019 (Figure 4) was the result of the hacking of a Business Associate. It involved one of the country's largest patient collections recovery agencies that had its patient information accessed by an unauthorized party. The breach was discovered when analysts found personal identifiable information (PII), including date of birth (DOB), Social Security Numbers, and physical addresses for sale on the dark web. Hackers appeared to gain access to patient information through the online patient portal over the course of several months, beginning in September 2018 and continuing until March 2019. This hacking incident affected 20,949,600 patient records, with 11,900,000 affected records from just one client.

INSIDER INCIDENTS CONTINUE TO DECREASE, SHOWING PROMISE WITH ADOPTION OF HEALTHCARE COMPLIANCE ANALYTICS

Overall, the number of insider-related incidents has decreased year over year since 2016 (Figure 5), this is largely due to the adoption of healthcare compliance analytics in health systems across the country and improved employee education on how to prevent privacy violations. Even still, the number of affected patient records remains fairly consistent. As Figure 6 shows, the number of patient records affected by insider-related incidents increased when comparing 2018 to 2019 data (2,793,607 breached records in 2018).

Even with the decrease in the number of insider incidents, they still pose a significant threat with one insider-related incident going undetected for over seven years. In this particular incident, sensitive patient information was viewable to external audiences outside their system network. Potentially exposed information included patient name, medical record number, insurance information, appointment times, and procedure information. At this time, it does not appear this data has been used maliciously and the organization has corrected the system configuration. Several other insider-related incidents went undiscovered for three or more years, putting significant amounts of patient data at risk.

Insiders were responsible for 19% of the total number of breaches in 2019, which is a slight decrease from the proportion in 2018 (28% of total incidents). There was information for 85 of those incidents, affecting 3,800,312 patient records (9% of total affected patient records).

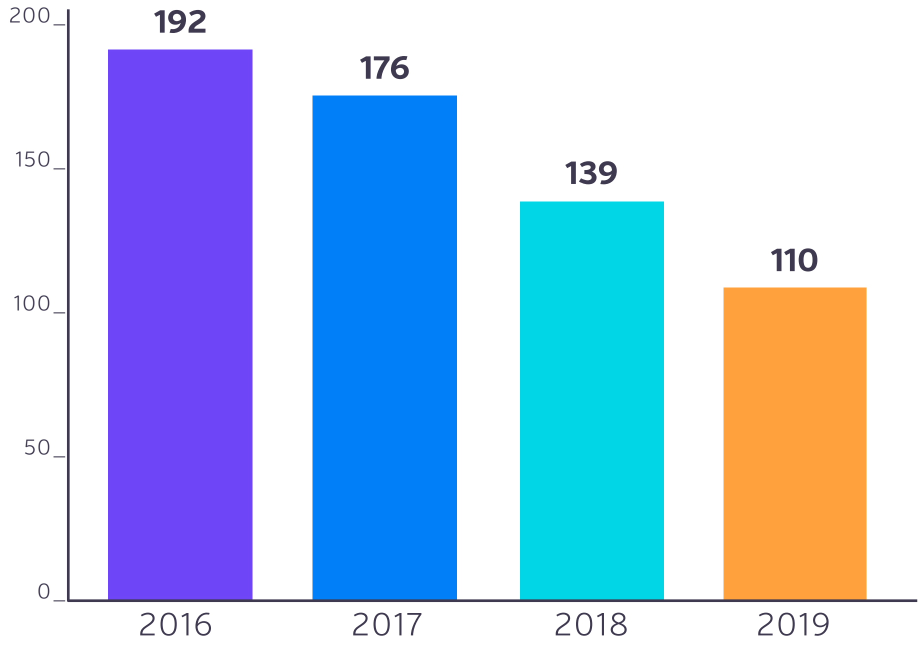


Figure 5. Total Insider-related incidents, 2016 - 2019 health data breaches

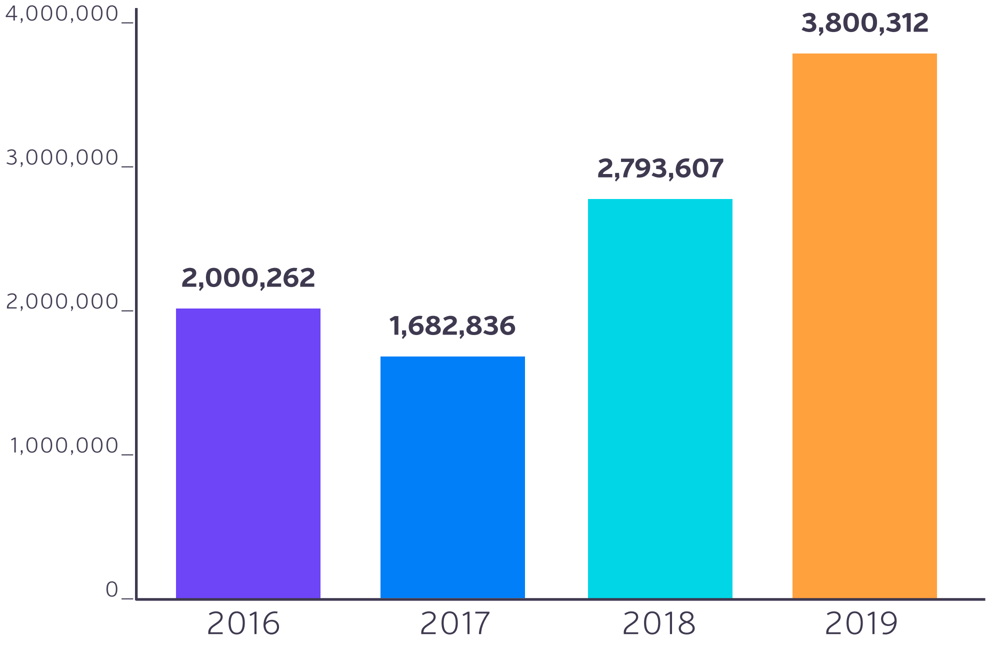
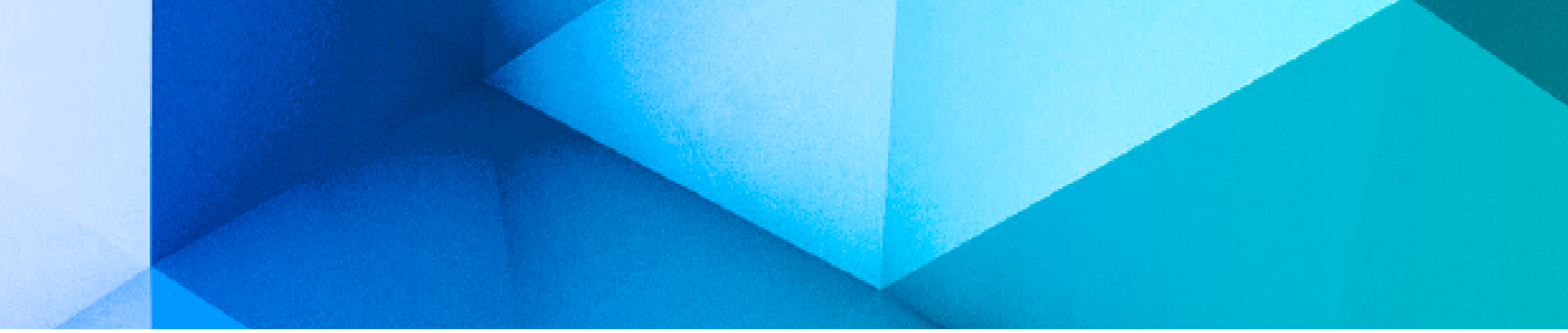


Figure 6. Number of breached patient records by insiders, 2016 - 2019 health data breaches



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 72 incidents that involved insider-error in 2019, and we have data for 59 of them. In contrast, 35 incidents involved insider-wrongdoing, and we have information for 26 of these incidents. It is important to note that there are two incidents for which there was not enough information to classify them as either insider-wrongdoing or insider-error. Insider-error affected 3,659,962 patient records and insider-wrongdoing affected 136,566 records. Figure 7 highlights that significantly more patient records were breached by insider-error than by insiders with malicious intent.

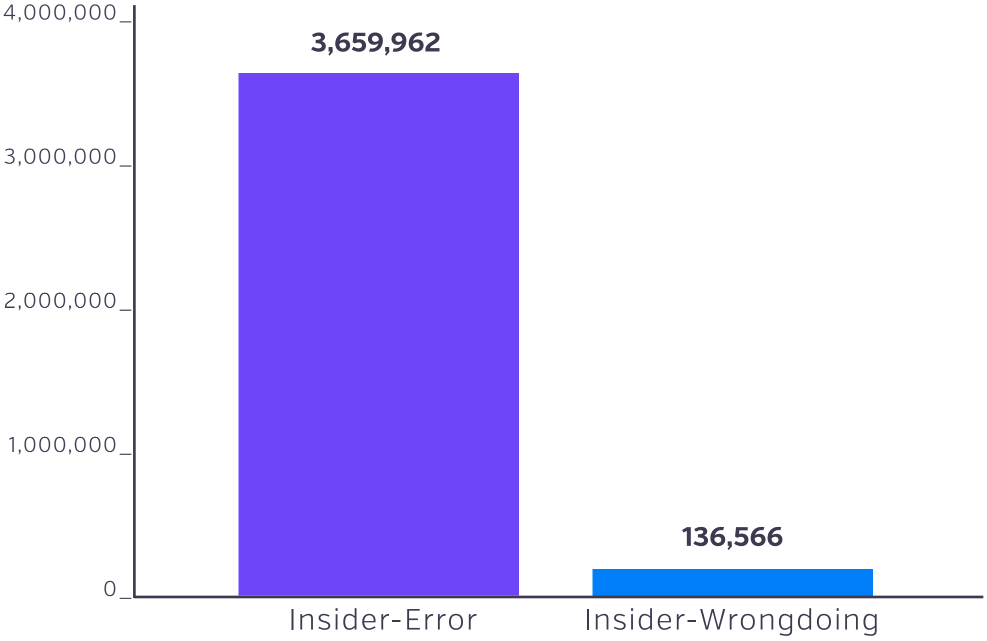


Figure 7. Number of patient records breached by insiders, 2019 health data breaches

While there were substantially fewer patient records breached by insider-wrongdoing, they are often more dangerous since employees with legitimate access to patient information can abuse their access with malicious intent, often undetected. In one recent case from 2019, a nurse is suspected of gaining access to patient information and providing the data to a third-party for fraudulent purposes. The Maryland-based healthcare organization discovered the breach when law enforcement reached out after the employee's associate was arrested for an unrelated matter. It is estimated that 16,542 patients could have been affected over the course of almost two years (644 days) before discovery. Based on information provided by state and local law enforcement, the organization fired this employee and reported the incident to the Board of Nursing. The investigation is still ongoing.

This is just one example of the harm insider threats pose when employees, business associates, or vendors abuse their access to sensitive data while working for healthcare organizations. In addition to the loss of patient trust, this entity may now face substantial post-breach costs that have been estimated to be close to $10M per breach. As this example illustrates, insider threats can remain undetected for long periods of time due to their legitimate access, as described in an example above. Available technology, like healthcare compliance analytics, can leverage artificial intelligence (AI) to detect when insiders inappropriately access patient information and can potentially prevent these incidents in the future.

Hacking Incidents Affect an Alarming Number of Patients

The healthcare industry experienced yet another alarming increase in hacking incidents in 2019. As Figure 8 illustrates, the increase is consistent with a worrisome year over year trend since 2016. As Figure 9 illustrates, hacking incidents were relatively constant throughout the year, with a total of 330 incidents in 2019, comprising 58% of all 2019 breaches (Figure 10). We have data on 297 of those incidents, which affected 36,911,960 patient records (Figure 11). For comparison, in 2018, there were 222 hacking incidents, which affected 11,335,514 patient records (Figure 12).

It appears hacking incidents, particularly ransomware incidents, are on the rise; hackers are getting more creative in how they exploit healthcare organizations and patients alike. In contrast to previous hacking incidents, current ransomware threat actors have taken to naming victims who do not pay the ransom demands, and then publicly dumping the data if they refuse to pay.

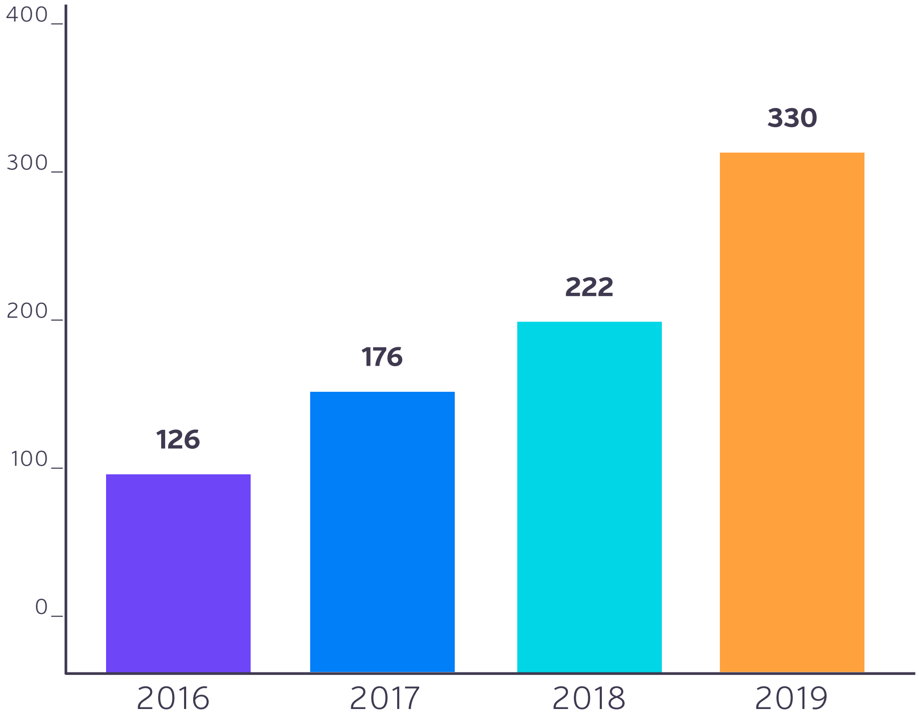


Figure 8. Total hacking incidents, 2016 - 2019 health data breaches

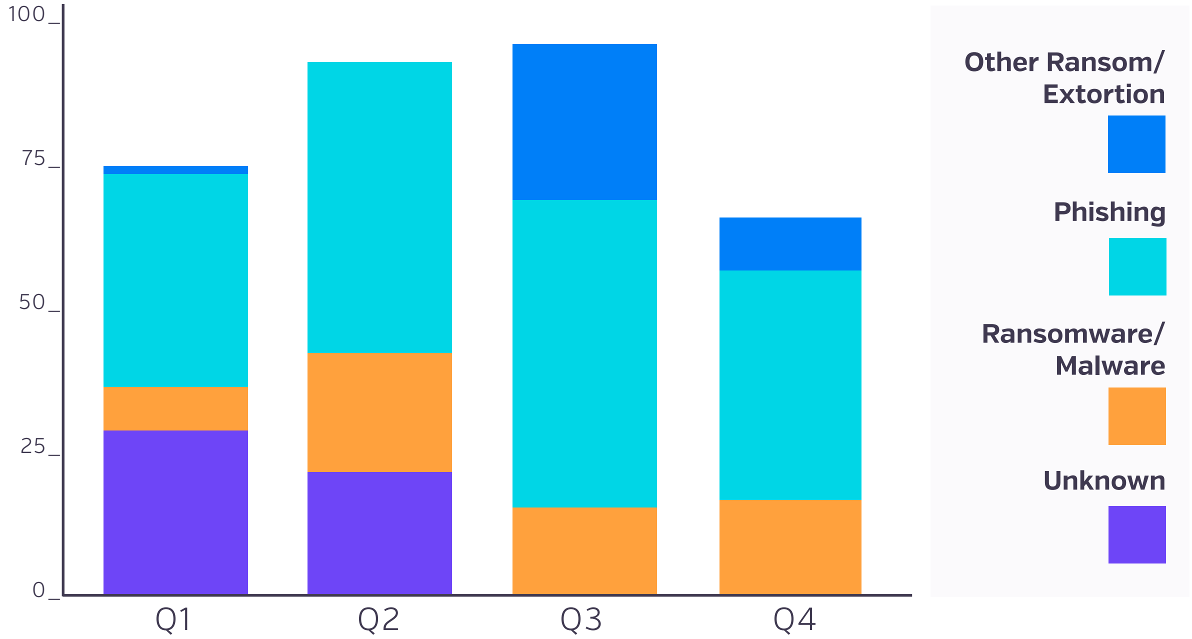


Figure 9. Total hacking incidents, 2019 health data breaches

To make matters worse, in 2019 there were incidents of hackers attempting to extort money from the breached patients, not just the affected healthcare organizations. In one incident in Florida, the hackers gained access to patient information and made the typical ransom demand of the breached organization. In a new malicious move, the hackers also sent ransom demands to a number of the affected patients, "threatening the public release of their photos and personal information unless unspecified ransom demands are negotiated and met." The FBI is currently investigating this incident. The healthcare industry should pay particular attention to these new types of threats in 2020.

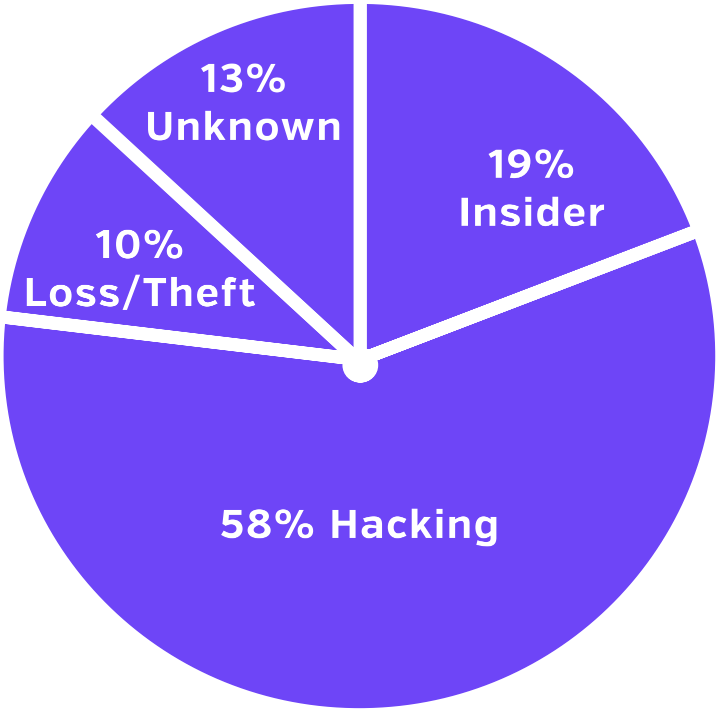


Figure 10. Type of incidents, 2019 health data breaches

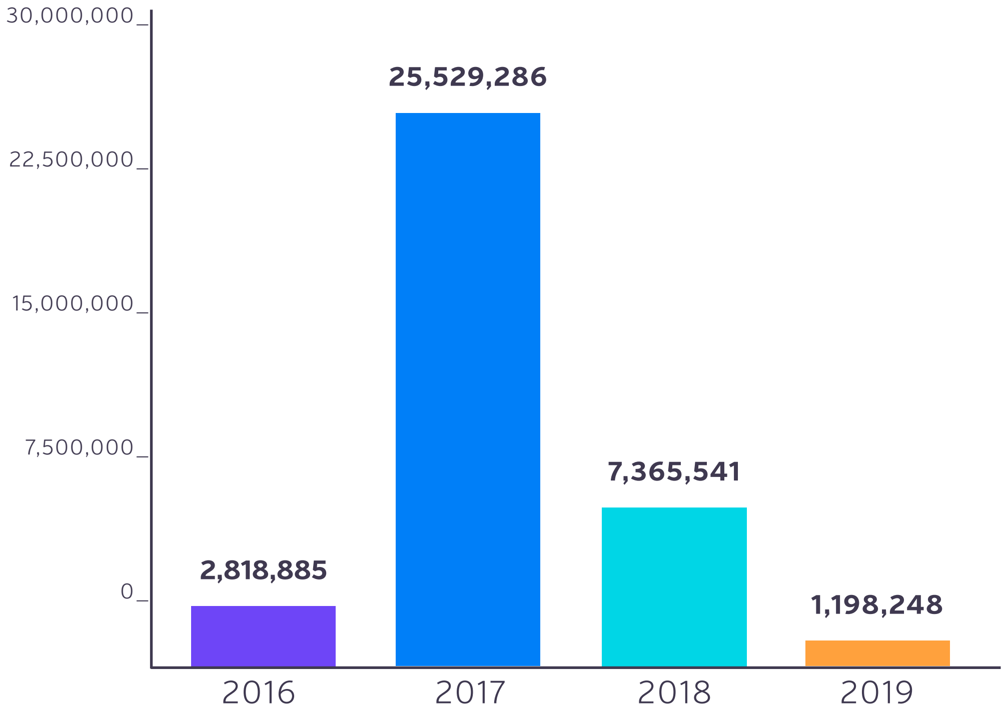


Figure 11. Patient records breached by hacking, 2019 health data breaches

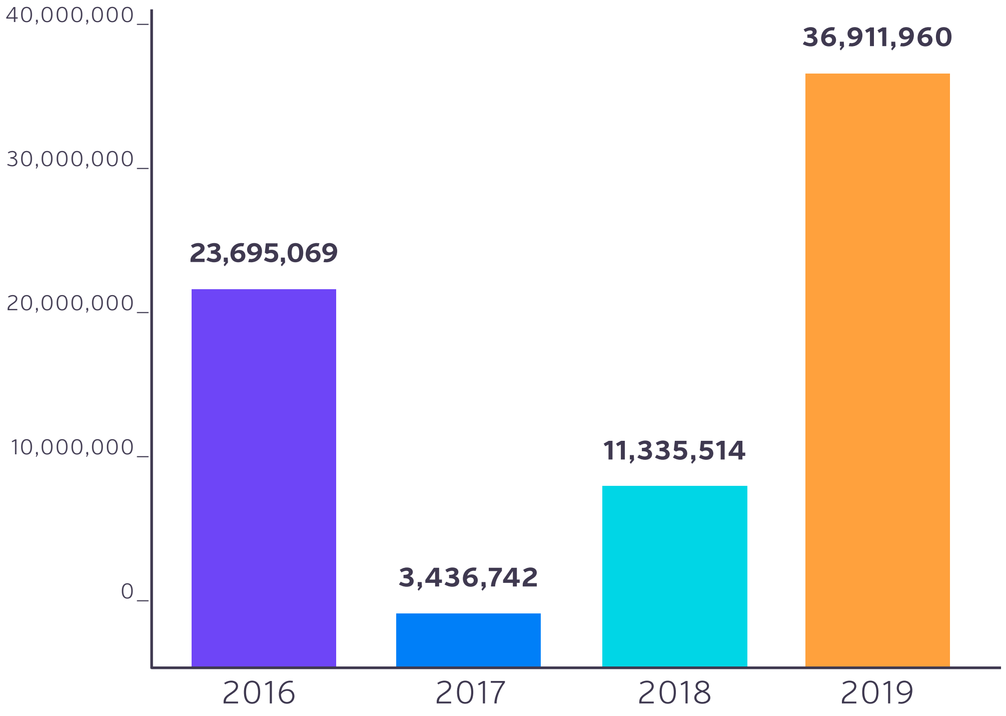


Figure 12. Patient records breached by hacking, 2016 - 2019 health data breaches

1,000,000,000 Radiology Images Exposed Online

For healthcare organizations to get ahead of these hackers, risk assessment and employee training and education are paramount. Organizations need to ensure they are testing to make sure the appropriate security measures in place are working as intended and that backups are separated from the main network so an attack cannot spread to the backups as well. This vulnerability became evident in 2019 when there were 1 billion radiology images that were not properly secured and were exposed online.

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 43 breaches due to theft. We have data for 41 incidents, which affected 370,124 records. Fourteen incidents involved missing or lost records, which affected 74,378 patient records.

Finally, there were 75 incidents that could not be categorized due to insufficient information. We have numbers for 66 such incidents, affecting 246,888 records.

Business Associate Involvement Breached 24M Patient Records

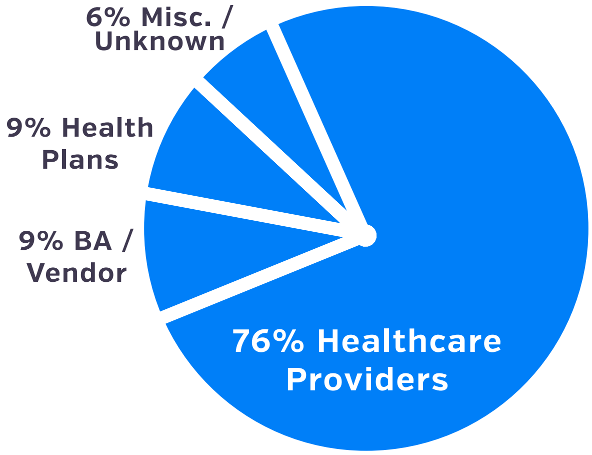


Fig 13. Types of entities reporting, 2019 health data breaches

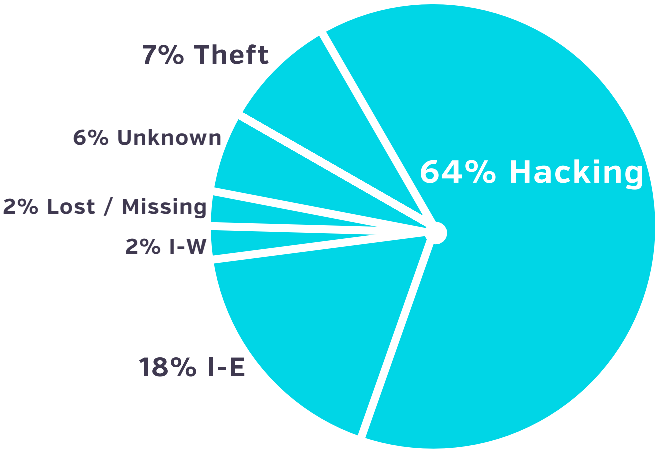


Fig 14. BA/third party involvement, 2019 health data breaches

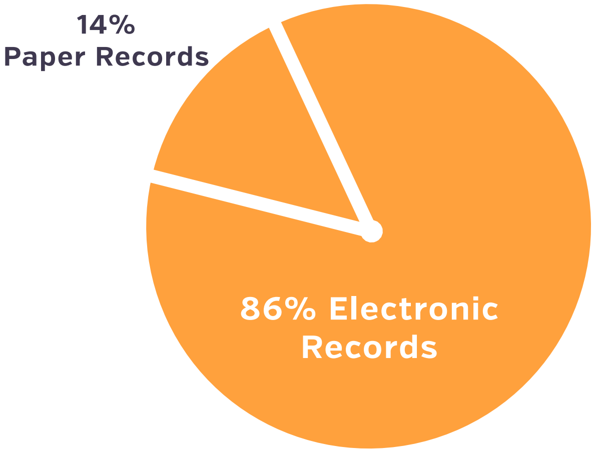


Fig 15. Paper vs. electronic records, 2019 health data breaches

Of the 572 reported incidents in 2019, 432 involved healthcare providers (76% of all reporting entities), 52 involved health plans (9%), 51 involved a business associate (9%), and 37 (6%) involved some other type of entity (Figure 13).

For the purpose of this report, Business Associates (BA) are defined as third-party vendors that are 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, 24,254,711 patient records were affected. Figure 14 shows that hacking incidents involved the largest proportion of BAs (64% of BA-involvement), followed by insider-error. Even with the large increase in affected patient records from BA-involved incidents, it should be noted that there could be 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, 79 incidents involved paper records (14% of total incidents, Figure 15). These incidents affected 408,714 patient records. It is possible that there are more breaches involving paper records, but again, some reports lacked sufficient detail to make that determination.

Several Insider Incidents Took Over Four Years to Discover

As illustrated in Figure 16, it took an average of 224 days for a healthcare organization to discover that it had suffered a breach in 2019. This represents an improvement from 2018, when it took an average of 255 days for breach detection. The median discovery time in 2019 was 44 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 3,164 days (8.7 years).

Of the 187 health data breaches for which we have data, it took an average of 80 days for organizations to report a breach to HHS, the media, or other sources after it was discovered (Figure 17). The average increased slightly when compared to 2018 data with an average of 73 days for reporting. The median disclosure time was 60 days, which is within the HHS required 60-day reporting window.

In addition, the data set for this analysis varies greatly from month to month, and data wasn't available for every incident that occurred in 2019. As a result, the smaller data set may not provide a complete picture of reporting times throughout the year. It's important to note that our analyses are not confined to HIPAA-covered entities who would be required by law to comply with the 60-day notification rule.

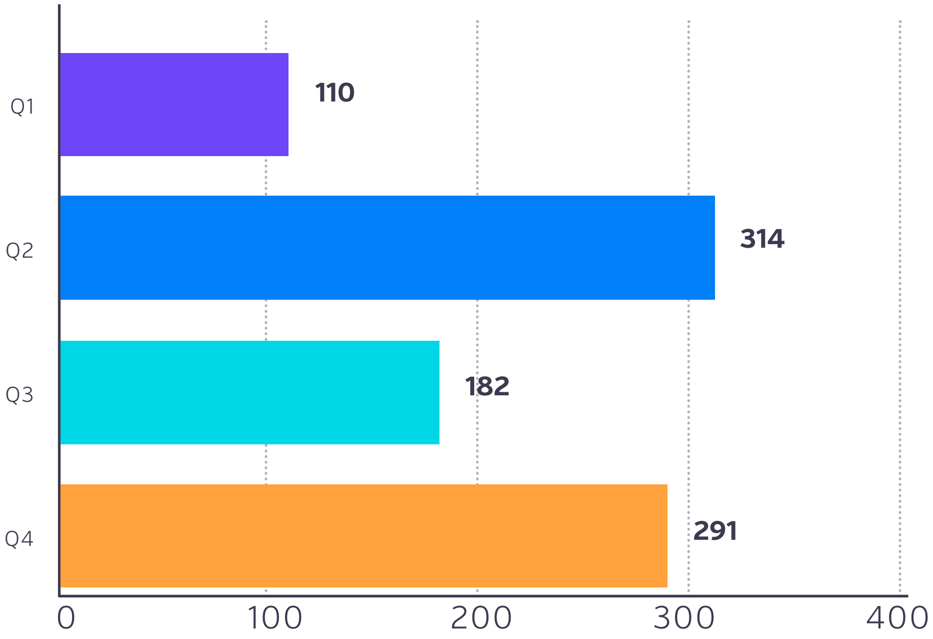


Figure 16. Average number of days from breach to discovery, 2019 health data breaches

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.

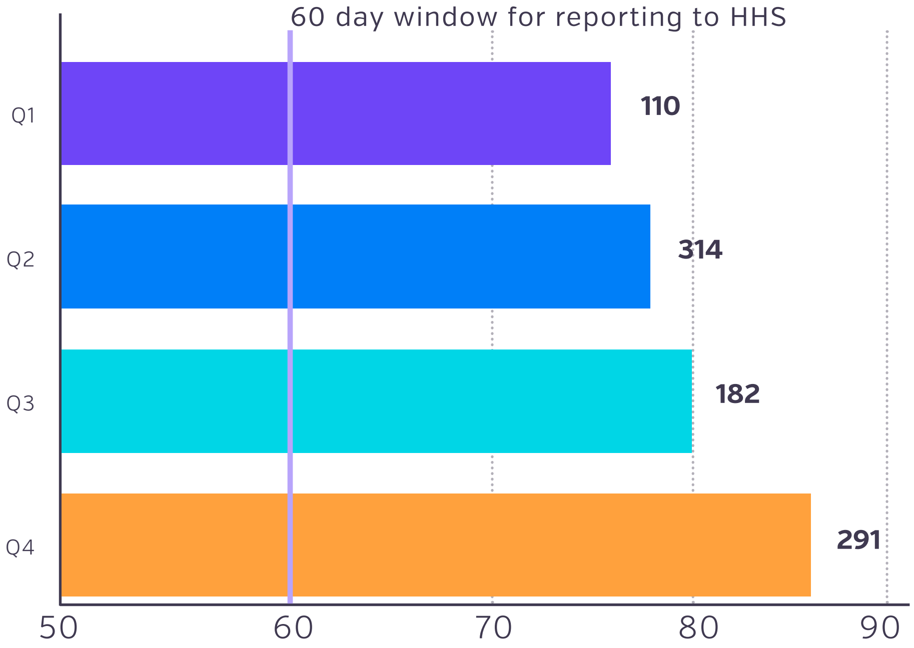
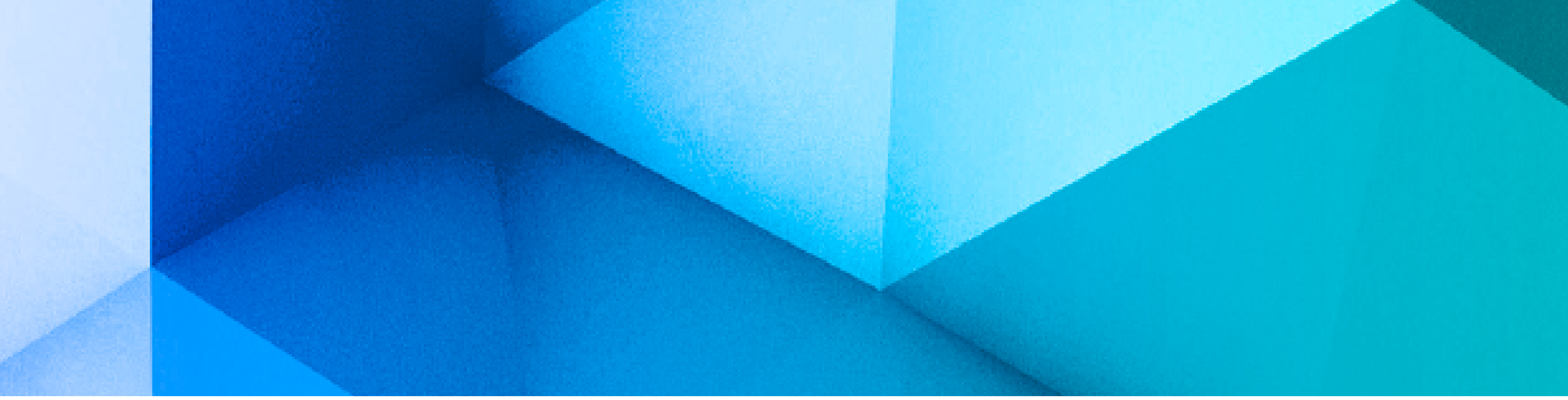


Figure 17. Average number of days from discovery to reporting to HHS, 2019 health data breaches



State Frequency

Forty-eight states (96%) are represented in the 570 incidents for which we had location data. Two incidents did not have enough information to determine their location, and two states did not have any reported breaches: North Dakota and New Hampshire. Texas had the most reported incidents with 59, followed by California with 49. Please note that numbers for some states are inflated because the analysis uses the state where the BA/vendor is located, not where the client is located.

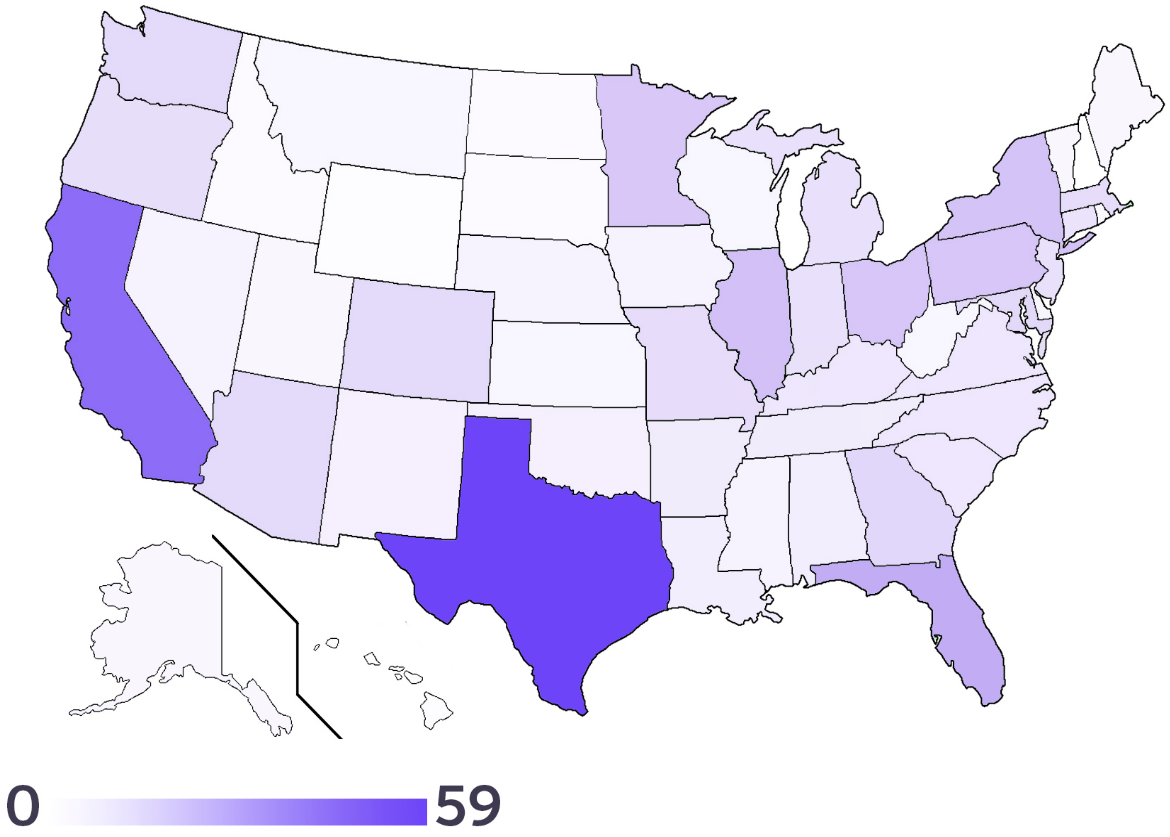


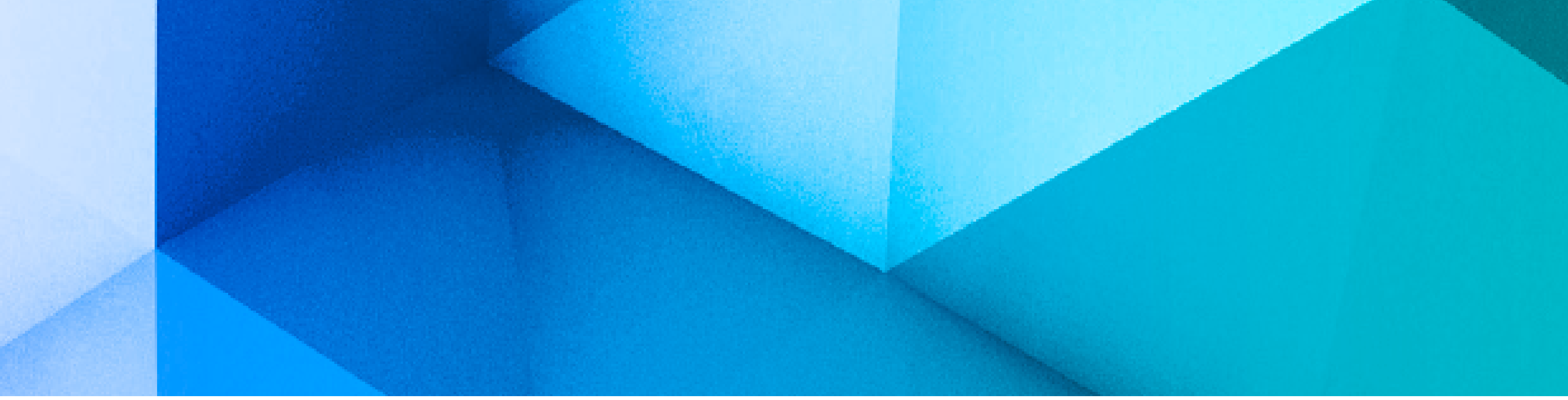
Figure 18. Number of incidents by state, 2019 health data breaches

Conclusion

As we have reported each year since 2016, healthcare continues to be highly targeted by hackers and other malicious actors, with the trend of at least one data breach per day continuing throughout the year. There was a notable increase in breach incidents; the number of affected patient records nearly tripled. We expect this trend to continue into 2020.

In fact, we may continue to see an increase in the number of incidents reported to HHS next year. The industry is getting better at breach detection by using healthcare compliance analytics to reduce overall risk to their organizations, but phishing techniques are of concern and continue to be popular with hackers. Hospital employee education and training to detect and not fall victim to such attacks are imperative to get ahead of the hacking incidents currently plaguing healthcare. Hackers are also using credential-stuffing attacks, making it increasingly important to train employees not to reuse passwords across work settings and personal accounts.

In 2020, it is vital that health systems make health data security a top priority, gaining insight into how patient data moves through the organization and the ability to differentiate between appropriate and inappropriate access to patient information. Armed with the latest information and utilizing the latest advances in technology, the healthcare industry can gain visibility into patient data access which will ultimately make their institutions more secure and further ensure patient trust.



About Protenus, Inc.

Protenus is a healthcare compliance analytics platform that uses the latest big data techniques and Protenus-led advances in data science, artificial intelligence, visualization, and software engineering to detect inappropriate activity in hospital EHR systems. The Protenus platform uniquely understands the clinical behavior and context of each person accessing patient data to determine the appropriateness of each action, elevating only true threats to privacy, security and compliance teams. Protenus and its partner health systems are fundamentally improving the way hospitals protect their patient data—further ensuring trust in healthcare.

About Databreaches.net

DataBreaches.net is a web site 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, 2019 and December 31, 2019. 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 ON 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.

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 their 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 2019, 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 there was protected health information 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 business associates 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 business associate 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 Business Associate 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 business associate 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 contact@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.

IN THE MEDIA

CBS THIS MORNING

U.S.News & WORLD REPORT

engadget

CBS NEWS

PROTENUS

2020

BREACH BAROMETER

contact@protenus.com | protenus.com