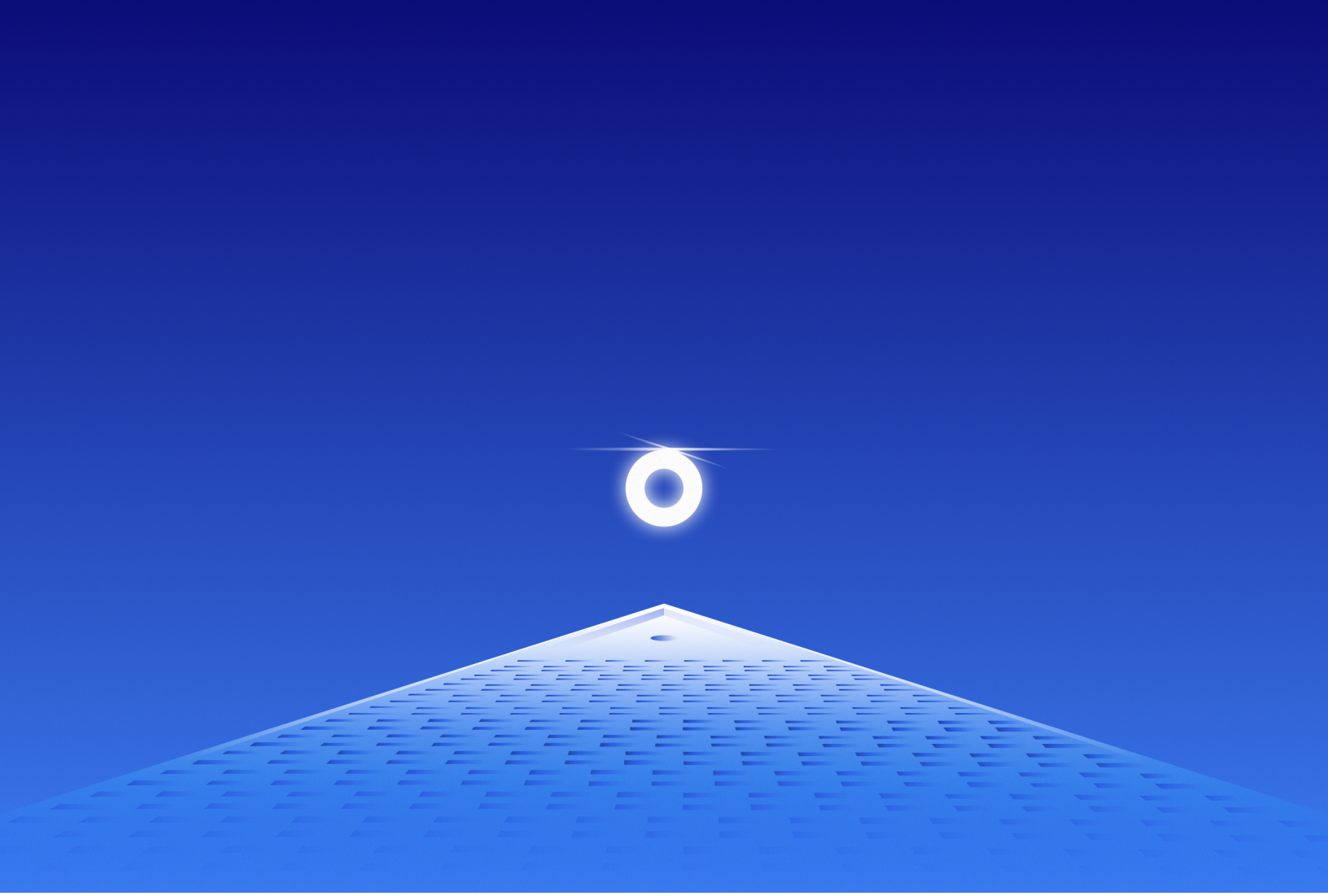


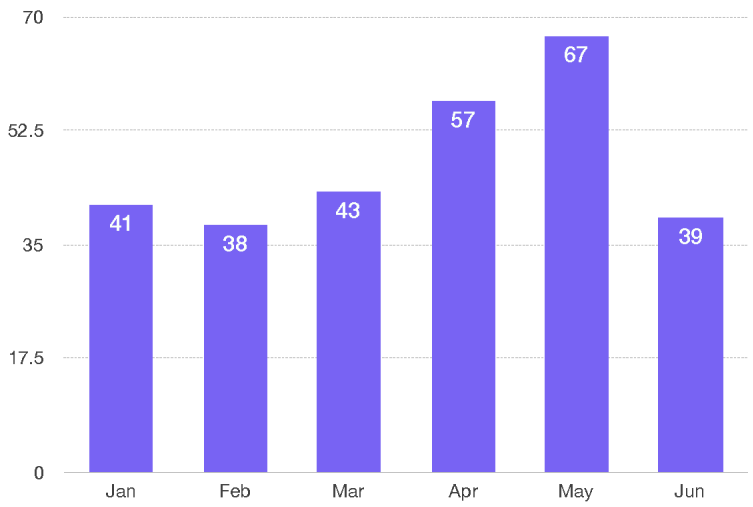
PROTENUS 2019 MID-YEAR BREACH BAROMETER

Breached Patient Records in First Half of 2019 Double the Total for All of 2018

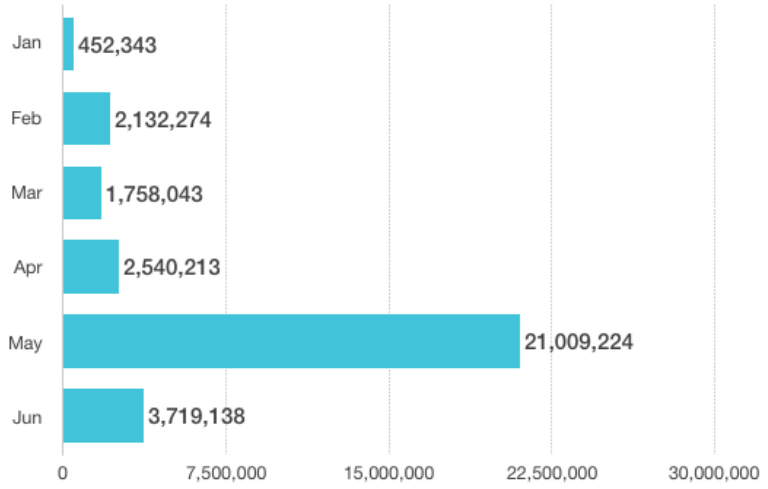
Protenus, Inc. in collaboration with DataBreaches.net

Overview

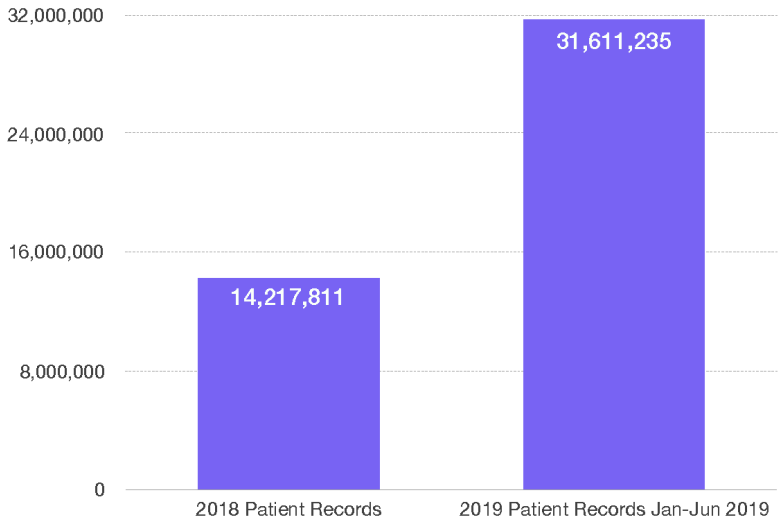
Breaches of patient privacy continue to loom throughout the healthcare industry and seem to be on the rise in the first half of 2019, with 285 incidents disclosed to U.S. Department of Health and Human Services (HHS) or the media from January to June 2019. Details were disclosed for 240 of these incidents, affecting 31,611,235 patient records. Alarmingly, the number of affected patient records is already more than double what the industry experienced throughout the entire year of 2018. This data reinforces the need for health systems to build privacy programs that review 100% of accesses to patient data in order to prevent these breaches from occurring, saving organization and patients significant post-breach costs.



Number of breach incidents disclosed, 2019 health data breaches



Number of affected patient records in disclosed incidents, 2019 health data breaches



Number of affected patient records in disclosed incidents, 2018 vs. 2019 health data breaches

The single largest breach in the first half of 2019 was a hacking incident affecting over 20M patient records that involved a medical collection agency.

The incident was discovered when patient data was found for sale on the Dark Web. The hackers potentially gained access to patients' social security numbers, dates of birth, and physical addresses. This incident affected multiple large entities including Quest Diagnostic, LabCorp, and Optum 360. Law enforcement has been involved and further investigations are currently taking place.

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	20,522,600
June	Health Plan	Hacking	2,964,778

Largest disclosed incidents, Jan - Jun 2019 health data breaches

Hospital insiders responsible for breaching 3M+ patient records

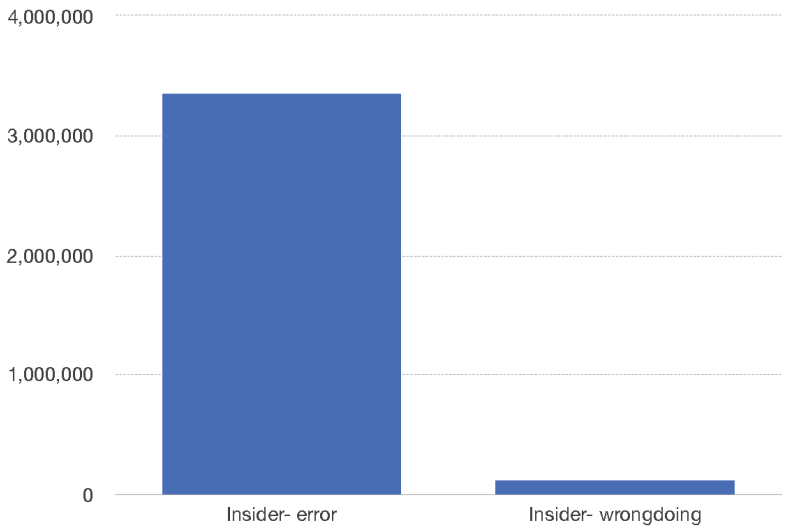
For incidents disclosed to HHS or the media, insiders were responsible for 20.91% of the total number of breaches in the first half of 2019 (60 incidents). Details were disclosed for 47 of those incidents, affecting 3,457,621 patient records (11% of total breached patient records).

For the purposes of our analysis, insider incidents are characterized as either insider-error or insider-wrongdoing. The former includes accidents and other incidents without malicious intent that could be considered "human error."

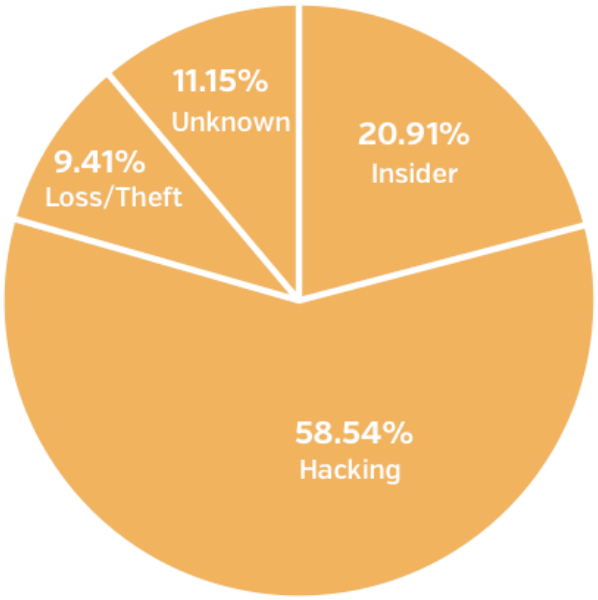
Insider-wrongdoing includes employee theft of information, snooping in patient files, and other cases where employees appeared to have knowingly violated the law.

There were 35 publicly disclosed incidents that involved insider-error between January and June 2019. Details were disclosed for 29 of these

incidents, affecting 3,346,145 patient records. In contrast, 22 incidents involved insider-wrongdoing, with data disclosed for 18 of these incidents. The substantial number of insider-related incidents should serve as a reminder for healthcare organizations to prioritize routine training and 100% activity auditing and documentation for their workforce. Recurring education is instrumental in ensuring healthcare employees are aware of common threats to patient privacy and how to prevent them, helping reduce to reduce risk across the entire organization. Auditing and documentation is essential to hold individuals accountable to this training.



Patient records breached by Insider-error vs. Insider-wrongdoing, 2019 health data breaches



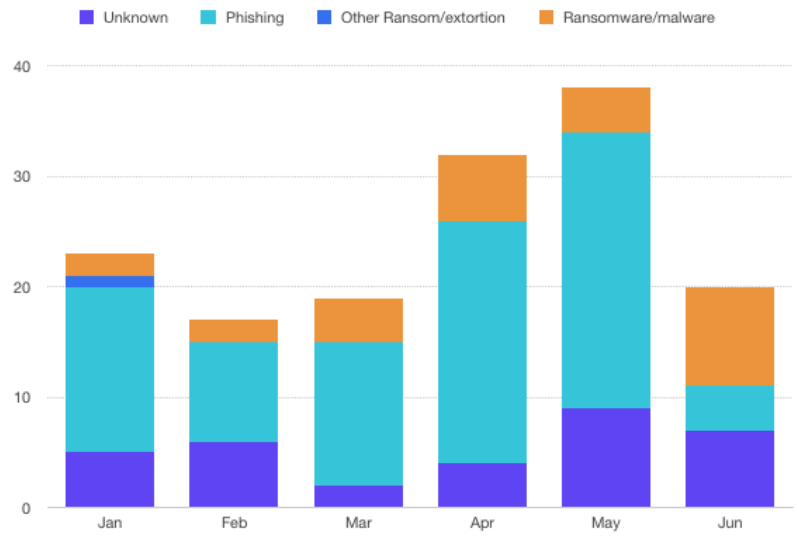
Type of disclosed incidents, 2019 health data breaches

Hacking responsible for 88% of breached records between January and June

Hacking continues to threaten healthcare organizations, with a distressing number of patient records breached in the first half of the year. Between January and June, there were 168 hacking incidents (59% of all publicly disclosed incidents). Details were disclosed for 135 of those incidents, which affected a staggering 27,819,320 patient records. 27 of those reported incidents specifically mentioned ransomware or malware, 88 incidents mentioned a phishing attack, and one incidents mentioned another form of ransomware or extortion.

In addition to malware, ransomware, and phishing, there were 24 reported incidents related to theft. Data was disclosed for 23 of those incidents, which affected 184,932 patient records.

Finally, there were 32 disclosed incidents in which not enough information was available to categorize them, affecting 142,009 patient records.

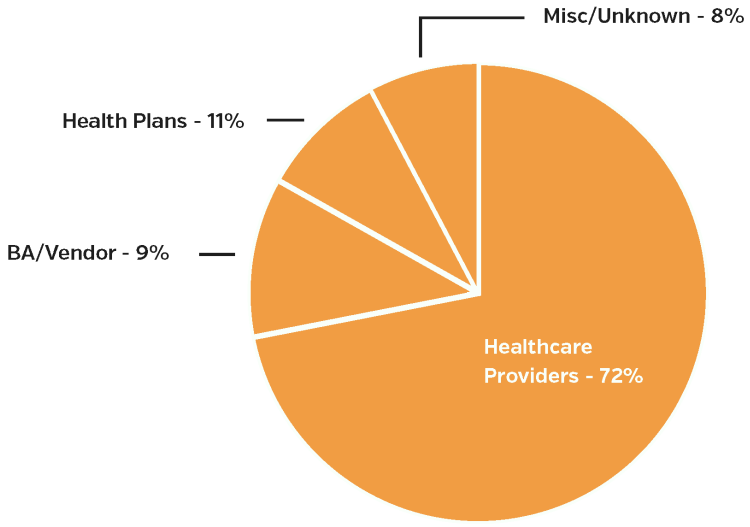


Disclosed hacking incidents, 2019 health data breaches

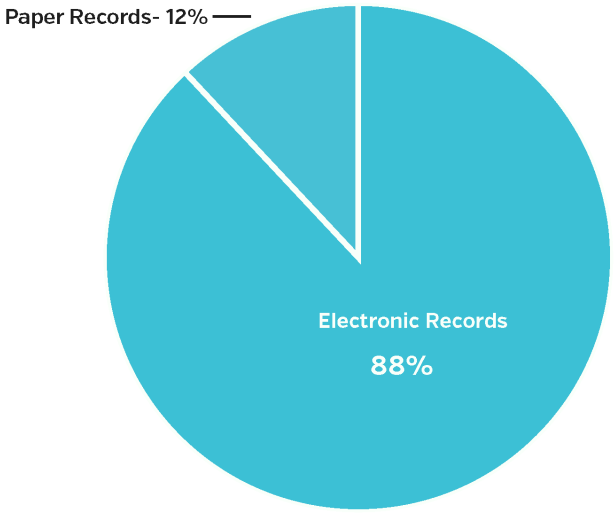
Majority of breaches to patient data occur in provider setting

Of the 285 disclosed health data breaches that occurred between January and June of 2019, 205 of them (72% of total incidents) were disclosed by a healthcare provider, 32 were disclosed by a health plan, 26 were disclosed by a business associate or third-party vendor, and 22 were disclosed by businesses or other organizations.

Even though most healthcare organizations have already switched over to digitized patient records, 35 breach incidents still involved paper records. Disclosed data was available for 30 incidents, affecting 84,906 patient records. There may have been more incidents in which paper or film records were involved, but some reports lacked sufficient information to make that determination.



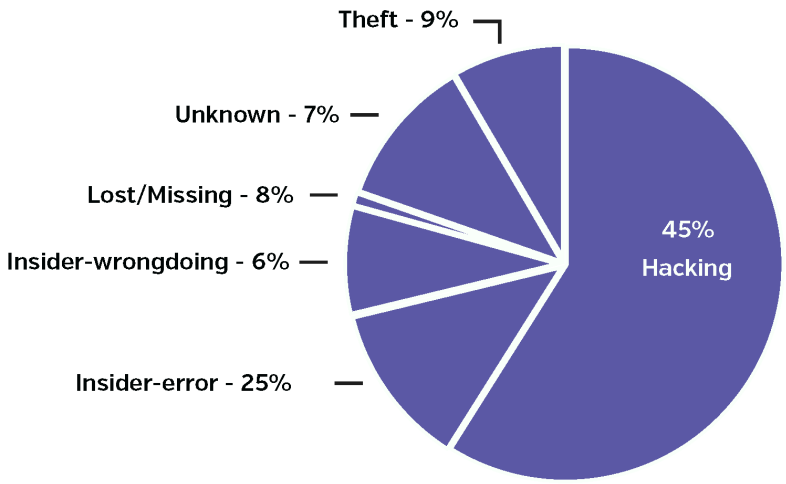
Type of entities disclosing, 2019 health data breaches



Paper vs. electronic medical records in disclosed breached, 2019 health data breaches

Hacking appears to be a significant challenge for Business Associates/Third-parties in early 2019

There were a total of 51 disclosed incidents that involved business associates (BAs) or third-party vendors (9% of total incidents). Information is available for 43 of these incidents, which affected 23,410,073 patient records (74% of total patient records). There were 31 instances in which a business associate was involved with a hacking incident, eight insider-error incidents, four insider-wrongdoing incident, four incidents of theft, and four incidents with unknown categorization. Nevertheless, it should be noted that there could be even more incidents involving third-parties, but there was not enough information to make that determination.



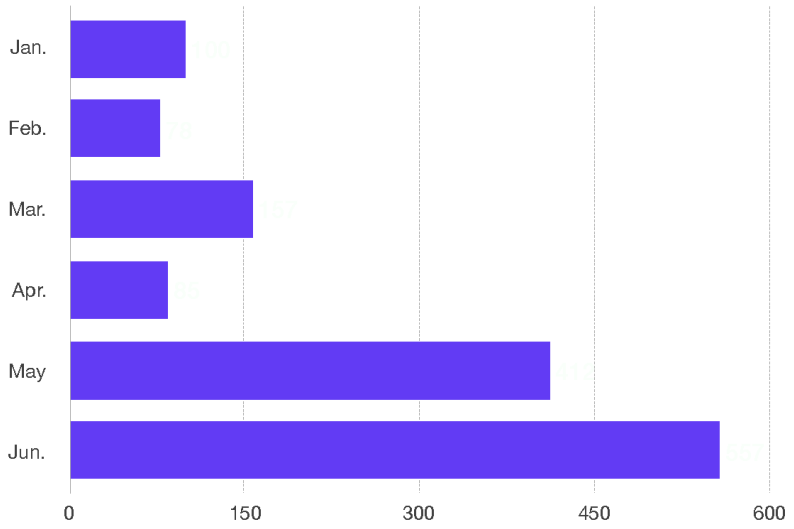
Business Associates or third-party involvement, 2019 health data breaches

One hacking incident took 8.5 years to discover

Of the 67 health data breaches for which data was disclosed, it took an average of 214 days to discover a breach had occurred. The median discovery time was 50 days. There were a wide variety of time frames for discovery,

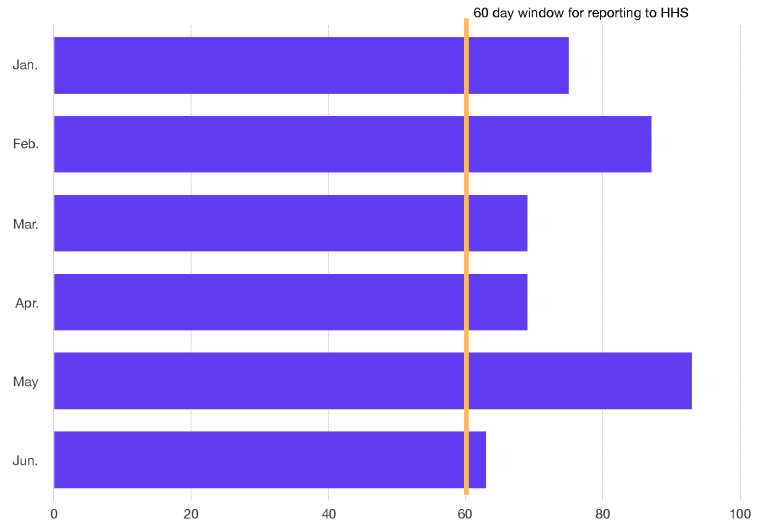
with the shortest discovery time of one day and the longest of 3,164 days (over eight years).

The longest incident to be discovered in the first half of 2019 was due to a hacking incident an insurer and administrator of dental and vision benefits. The incident occurred when an internal alert determined that an unauthorized party may have accessed some of its computer servers. The unauthorized access may have occurred as early as August 2010. It is believed that compromised patient information may include names, addresses, dates of birth, social security numbers, tax IDs, and various financial information. The incident was finally discovered in April 2019, affecting 2,964,778 patient records.



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

Of the 101 incidents for which data was disclosed, it took an average of 77 days from when a breach was discovered to when it was disclosed to HHS, the media, or other sources. The median disclosure time was 60 days. It is important to note that information is available for less than half of the breaches disclosed from January to June 2019, making it difficult to draw conclusions from the available data.



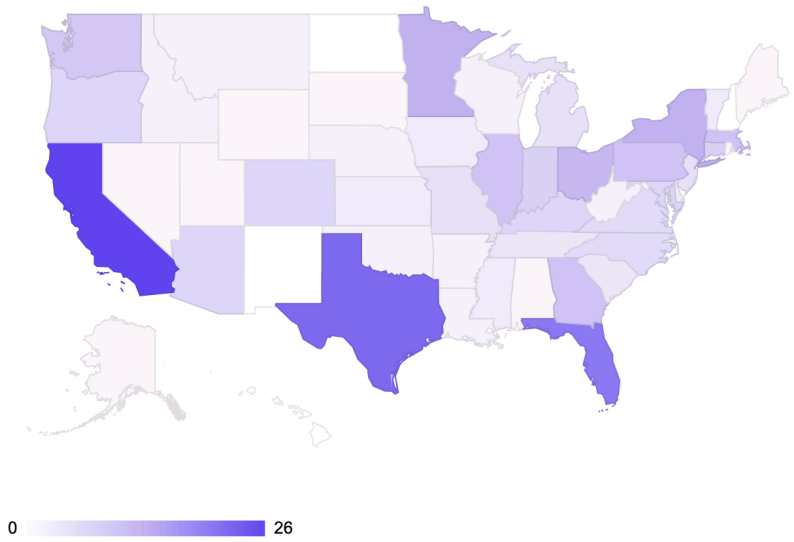
Average number of days from discovery to disclosure, 2019 health data breaches

With the exception of the longest-to-discover incident mentioned above, insider-related incidents generally take longer to discover. This is the case because insiders have legitimate reasons to access to the EHR, making it easier for inappropriate accesses to go under the radar. There were at least two other insider-related incidents where it took over 5 years to discover in the first half of the year. As mentioned above, the longest breach reported so far in 2019 went on for over eight years before it was discovered by the organization. This is not a standalone incident. Insider-related incidents are routinely reported to have longer than average detection times, making it imperative for healthcare organizations to utilize advanced methods for detecting inappropriate accesses to patient data.

California has the most data breaches per state

46 states are represented in the 285 disclosed health data breaches between July and September 2018 for which we had location data. California had the most data breaches of any state, with 26 separate incidents. Texas had the second highest number, with 22 separate disclosed incidents, followed closely by Florida with 20 incidents. It is important to note that California often has more reported breaches, which could be due to a higher number of reporting

entity and patient volume, and/or more robust reporting methods and procedures.



Number of disclosed incidents by state, 2019 health data breaches

Conclusion

The large volume of breached patient data is an alarming find in the first half of 2019, especially given that the mid-year total already exceeds the total for all of last year (15,085,302 vs. 31,611,235 patient records). The largest disclosed incident contributes significantly to this sharp increase in affected patient records and is an unfortunate example of the damage that can be done by hacking incidents that remain undiscovered over long periods of time. In order for healthcare organizations to reduce risk across their organization and to truly combat the challenges associated with health data security, it is critical for healthcare privacy offices to utilize healthcare compliance analytics that will allow them to audit every access to their patient data. Full visibility into how their data is being accessed will help healthcare organizations prevent data breaches from wreaking havoc on their organization and the patients who trust them with their personal information.

Methodology

The purpose of this section is to explain decisions that were used to guide our analyses.

Sources

Incidents included in the analyses for this report were compiled for Protenus by DataBreaches.net, and include:

- Incidents reported to HHS between January 1, 2018 – June 30, 2019 that appear on their public breach tool. Incidents reported to HHS before December 31 that were not added to the breach tool in time have not been included.

- Incidents that were reported to other federal or state regulators such as SEC filings or state-mandated notification to state attorneys general or consumer protection agencies;

- Publicly disclosed incidents involving U.S. organizations or entities that are not HIPAA-covered entities but that involved what would be considered protected health information under HIPAA;

- Incidents based on research by DataBreaches.net that may not have been reported to federal or state regulators.

Coding

In addition to going beyond HHS's public breach tool to find breach incidents, this report also uses significantly different coding and analysis than HHS's public breach tool, permitting analyses that are not readily conducted based on HHS's tool, as follows:

- HHS's "unauthorized access/disclosure" category was abandoned in favor of a more refined analysis that allowed us to do a deeper dive

into the rate and scope of insider/human error breaches vs. insider/intentional wrongdoing breaches.

- HHS's "Hacking/IT incident" led to further analysis of incidents reported in that category to determine if there was actually an external attack or if – as was the case in a number of incidents – entities were reporting being "hacked" when it might be more accurate to describe the incident as an unintended exposure of PHI on public FTP servers that researchers or others then accessed. In those cases, regardless of how the entity submitted the incident to HHS, our analysis coded those incidents as "insider-error," just as failures to restore firewalls after an upgrade that resulted in data acquisition were coded as "insider-error."

Calculating Time 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 something like a Twitter announcement that made the public aware that there had been an incident.

In some cases, we did not have exact dates, but only knew 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.

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, if the third party's identity was known. In cases where the third party's location could not be determined, the incident was assigned to the covered entity's state.

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 very, very large iceberg, and any patterns we see in publicly disclosed breaches may not mirror what goes on beneath the tip.