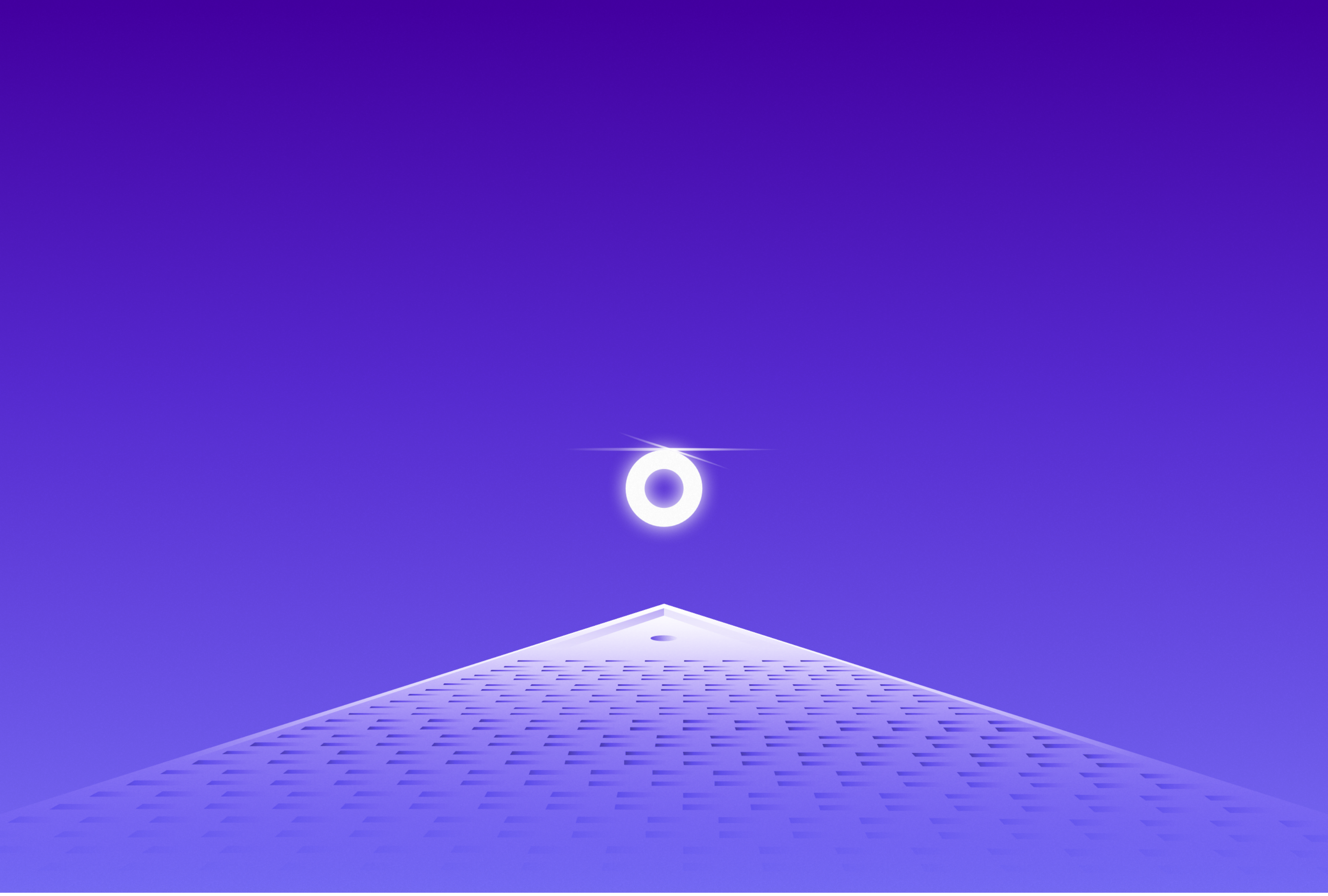


Q2 2018 PROTENUS BREACH BAROMETER

3.14M Patient Records Breached As Patients Are Increasingly Anxious About Health Data Security

Protenus, Inc. in Collaboration with DataBreaches.net

PROTENUS

Breach Barometer Snapshot

April – June 2018

142 disclosed health data breaches

3.14M breached patient records

3,917 average active EHR users per investigator

10.98 days, average time to case resolution

9.21 privacy violations per **1,000** employees

29.71% of violations were repeat offenses

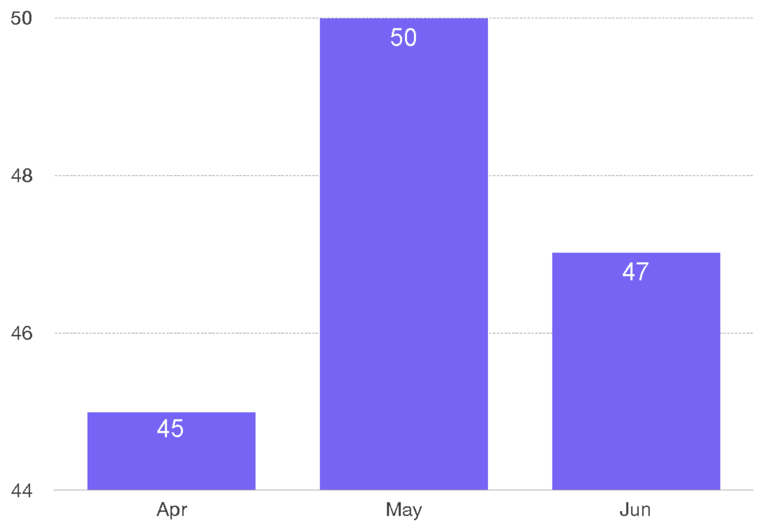
Family snooping most common insider-related breach

Overview

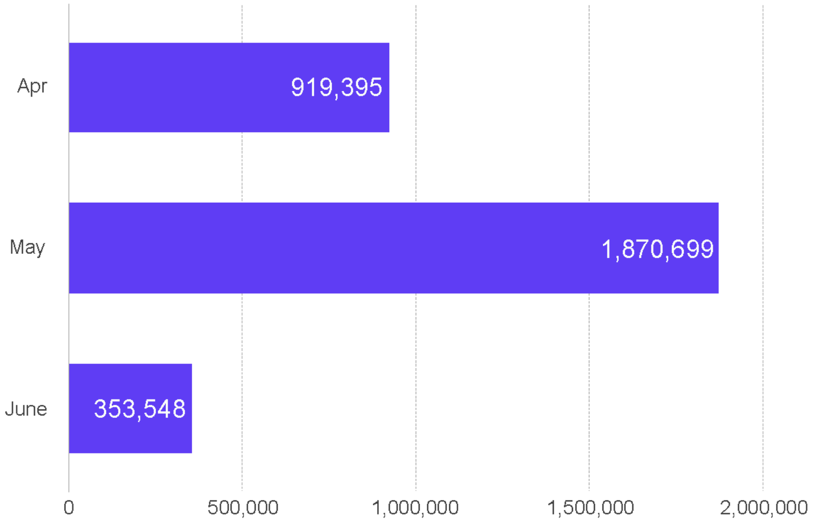
A recent study found that half of U.S. adults are "extremely or very concerned" about health data security, recognizing the sensitive nature of the information stored within a patient's medical record. Healthcare continues to suffer from routine health data breaches with a total of 142 incidents disclosed to U.S. Department of Health and Human Services (HHS) or the media from April to June (Q2) 2018. Details were disclosed for 116 of these incidents, affecting 3,143,642 patient records. The number of affected patient records almost tripled from those reported in Q1 2018 (1.13M patient records).

The single largest breach in Q2 2018 was a theft incident that involved a Sacramento-based office of the Department of Developmental Services, affecting 582,174 patient records. Burglars ransacked the office, damaged files and stole state property. The thieves also started a fire before leaving the premises, the sprinkler system responded accordingly and doused many of the patient records. Officials say personal information for 15,000 employees of regional centers, service providers, job-seekers, and parents of minors enrolled in various departmental programs was compromised by the burglary. This type of incident emphasizes that criminals know how sensitive and valuable medical information can be and will go to extreme lengths to steal patient data with the hopes of reselling it on the Dark Web for significant profit.

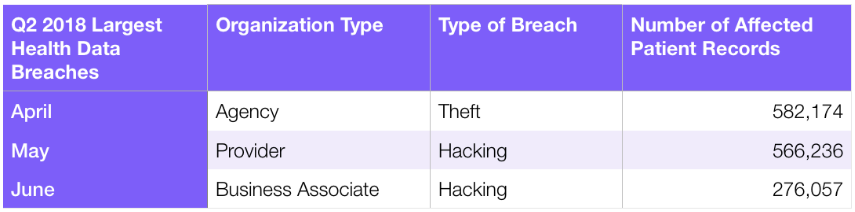
In addition to incidents disclosed to HHS or the media, this report compiles proprietary, non-public data on health data breaches nationwide in Q2 2018. The analysis involved a review of tens of trillions of individual accesses to electronic health records in Q2 2018 by Protenus, a healthcare compliance analytics platform used by health systems to audit access to health data.



Number of breach incidents disclosed, Q2 2018 health data breaches



Number of patient records in disclosed incidents, Q2 2018 health data breaches



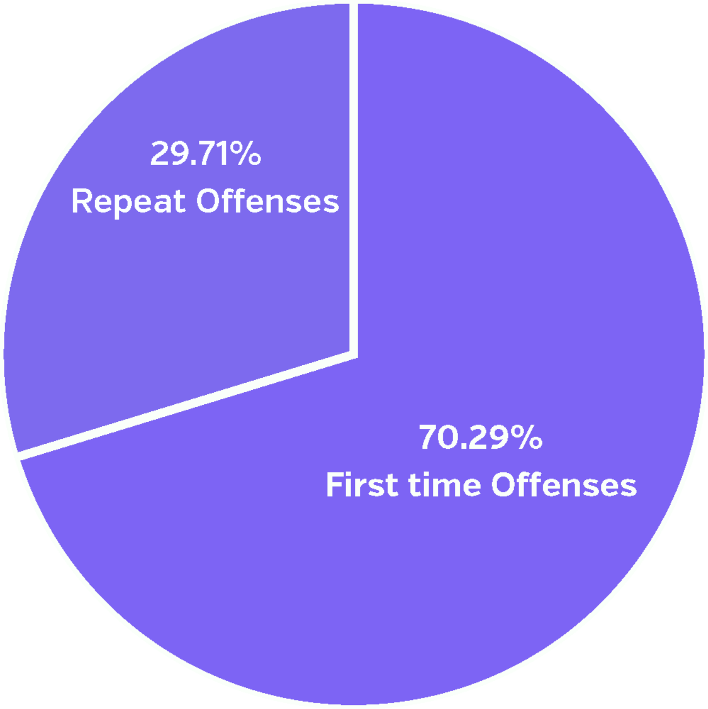
Q2 2018 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
April	Agency	Theft	582,174
May	Provider	Hacking	566,236
June	Business Associate	Hacking	276,057

Largest disclosed incidents, Q2 2018 health data breaches

Insiders continue to repeatedly breach patient privacy

In Q2 2018, 29.71% of privacy violations were repeat offenders. This evidence indicates health systems accumulate risk that compounds over time if proper reporting and education do not occur. On average, if an individual healthcare employee breaches patient privacy once, there is a greater than 30% chance that they will do so again in three months' time, and a greater than 66% chance they will do so again in a years' time. In other words, even minor privacy violations that are not promptly detected and mitigated, have the potential to compound risk over time.

Routine training and education are instrumental in preparing healthcare employees to prevent common threats to patient privacy. A study conducted in early 2018 found that 78% of staff lacked proper data privacy and security awareness. Resources provided to healthcare organizations are pivotal in reducing the number of breach incidents that occur. Educating and retraining workforce members on data privacy and security policy and procedures can reduce the frequency of repeat offenders within the organization.



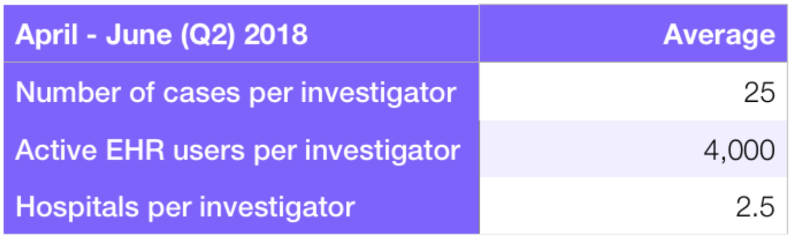
First time vs. repeat offenses to patient privacy, Q2 2018 health data breaches

In hospital teams responsible for responding to insider threats, one investigator monitors an average of nearly 4000 employees

Due to the daily volume of accesses to health data, privacy and security teams charged with reviewing and investigating breaches to patient privacy that occur within healthcare organizations are only able to investigate a small fraction of potential violations. Data available for Q2 2018 shows just how difficult it is for investigators to keep up with the volume of insider threats.

The Protenus platform scans hundreds of millions of accesses to patient records every quarter to detect anomalous activity, using AI-powered analytics to review every access to patient data. The data shows that each hospital investigator is responsible for monitoring the electronic access of an average of 4,000 active EHR users in Q2 2018, underscoring that manual audit processes, like ad-hoc or random audits, are insufficient to monitor such a large population, each of whom accesses multiple medical records per day.

Protenus data also found that each investigator is responsible for an average of 2.5 hospitals, which is down slightly from what was found in Q1. This decrease is a great sign that health systems are investing more into their privacy and security teams, enabling teams to better leverage resources to protect patient privacy.



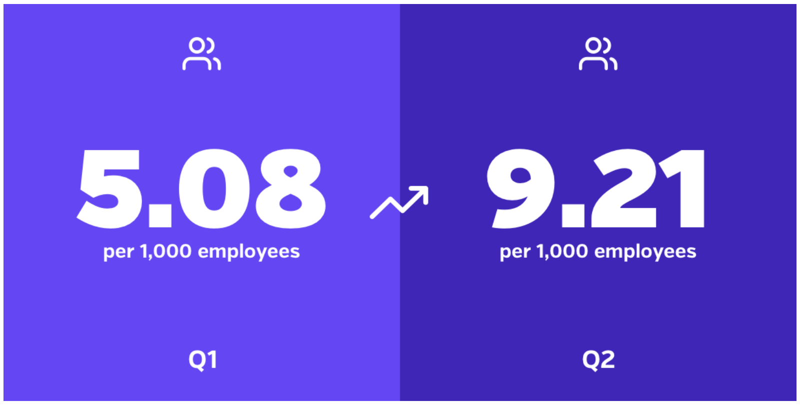
April - June (Q2) 2018	Average
Number of cases per investigator	25
Active EHR users per investigator	4,000
Hospitals per investigator	2.5

Averages for privacy investigators, Protenus data 2018

9 out of 1000 employees breach patient privacy, and family member snooping is the most common insider-related violation

For incidents disclosed to HHS or the media, insiders were responsible for 30.99% of the total number of breaches in Q2 2018 (44 incidents). Details were disclosed for 27 of those incidents, affecting 421,180 patient records (13.4% of total breached patient records).

Protenus data estimated that on average, 9.21 healthcare employees breach patient privacy per every 1,000 employees. This increase, from what was reported in Q1 2018, is due to healthcare privacy teams better leveraging advanced analytics, and proactively detecting more incidents.

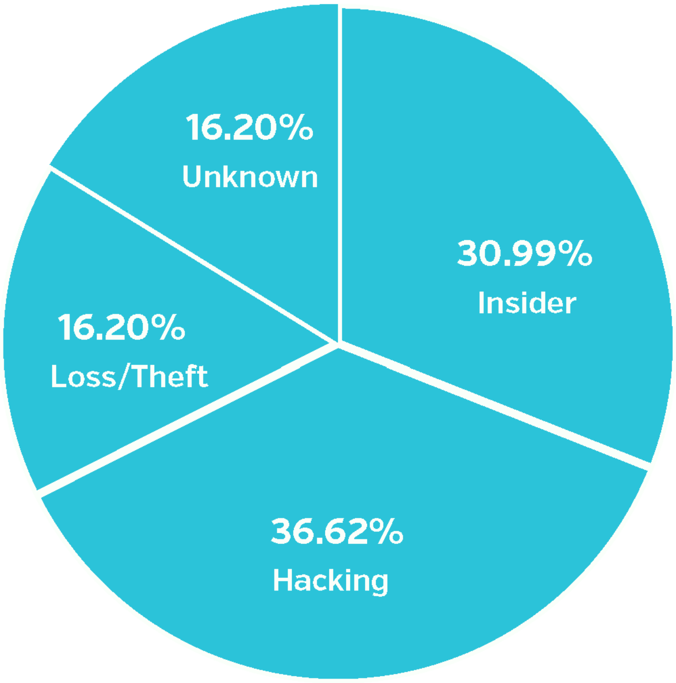


Average number of employees violating privacy per 1,000 employees, Protenus data 2018

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

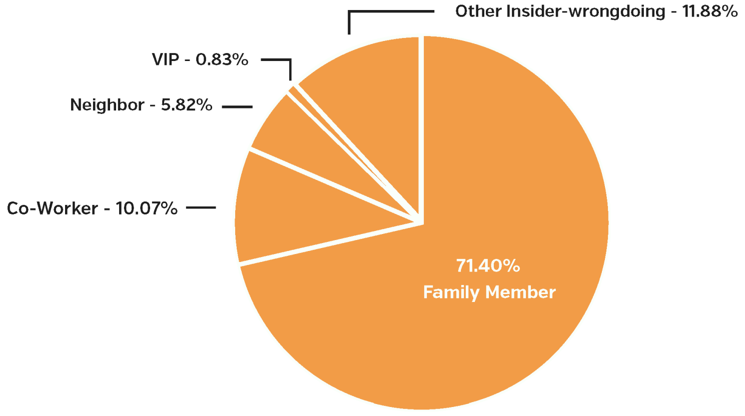
Insider-wrongdoing included employee theft of information, snooping in patient files, and other cases where employees appeared to have knowingly violated the law.

There were 25 publicly disclosed incidents that involved insider-error between April and June 2018. Details were disclosed for 14 of these incidents, affecting 343,036 patient records. In contrast, 18 incidents involved insider-wrongdoing, with data disclosed for 13 of these incidents. There was a substantial increase of breached patient records as a result of insider-wrongdoing. In Q1 2018, there were only 4,597 affected patient records, while in Q2 2018, there were 70,562 affected patient records.



Type of disclosed incidents, Q2 2018 health data breaches

The largest category of insider-related breaches in Q2 2018 involved healthcare employees snooping on their own family members (71.40% of violations). The "other insider-wrongdoing" category included less common, but often more malicious incidents like phishing attacks, insider credential sharing, downloading records for dale, identity theft, or other types of nefarious behaviors. This category of insider-wrongdoing (11.88% of violations) was the second most common insider-related violation, followed by snooping on fellow co-workers (10.07%) and snooping on their neighbors (5.82%). VIP-related incidents were less common, representing less than one percent (0.83%) of total insider-related incidents detected between April and June 2018. Protenus data also found that the median resolution time for insider-related incidents at healthcare organizations using AI-powered advanced analytics was 10.98 days, which can help health care organizations be more prepared to meet HHS reporting deadlines.



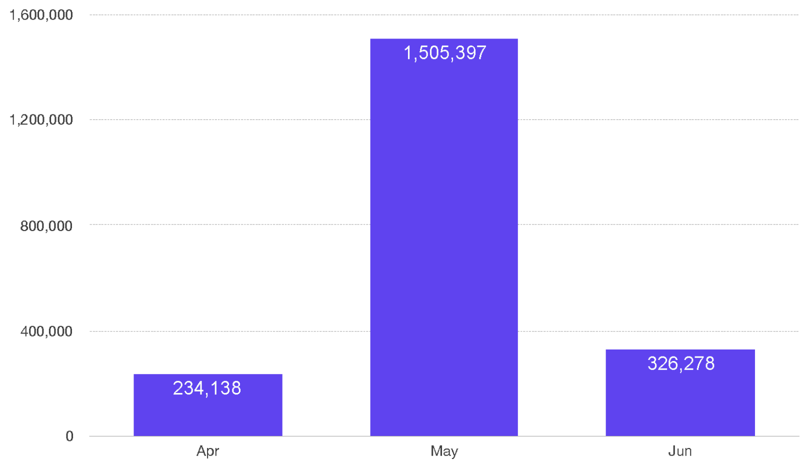
Insider incidents by category of violation, Q2 2018 health data breaches

Hacking incidents almost double from Q1 to Q2 2018

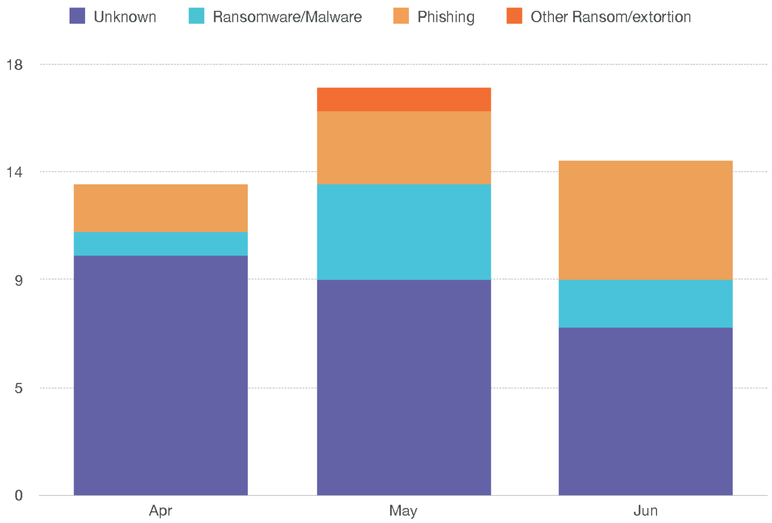
Hacking continues to threaten healthcare organizations in 2018, with an increase in incidents in the second quarter. Between January and March, there were 30 hacking incidents, however, between April and June 2018 there have been a total of 52 incidents (36.6% of all Q2 2018 publicly disclosed incidents). Details were disclosed for 44 of those incidents, which affected 2,065,813 patient records. Seven of those reported incidents specifically mentioned ransomware or malware, ten incidents mentioned a phishing attack, and one incident mentioned another form of ransomware or extortion.

In addition to malware, ransomware, and phishing, there were 23 reported incidents related to theft. Data was disclosed for 19 of those incidents, which affected 604,179 patient records.

Finally, there were 23 disclosed incidents in which not enough information was available to categorize them, affecting 52,470 patient records.



Patient records breached by disclosed hacking incidents, Q2 2018 health data breaches

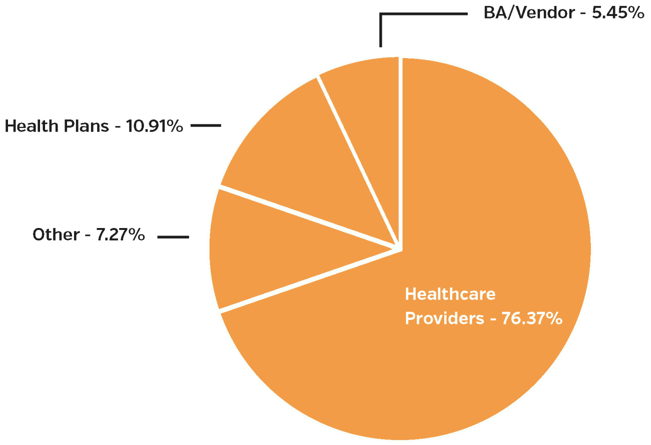


Disclosed hacking incidents, Q2 2018 health data breaches

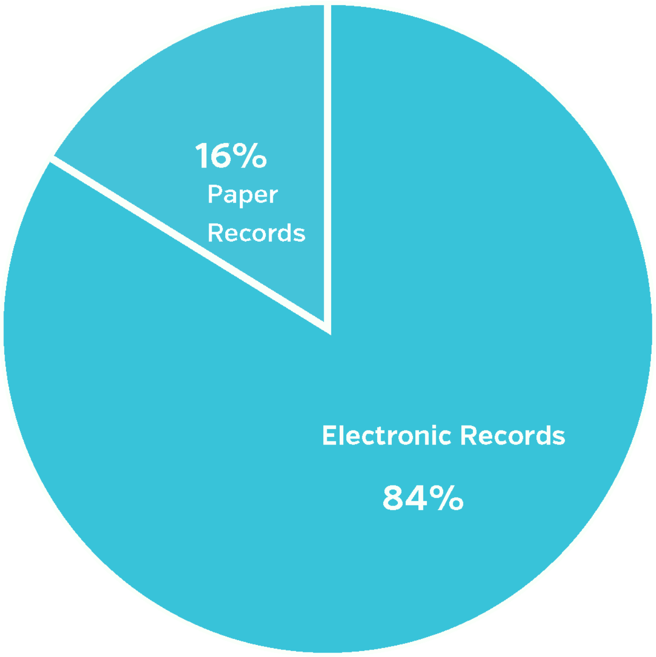
23 breach incidents still involved paper records

Of the 142 disclosed health data breaches that occurred between April and June of 2018, 99 of them (76.37% of total incidents) were disclosed by a healthcare provider, 15 were disclosed by a health plan, 18 were disclosed by a business associate or third-party vendor, and ten were disclosed by businesses or other organizations.

Even though most healthcare organizations have already switched over to digitized patient records, 23 breach incidents still involved paper records. Disclosed data was available for 14 incidents, affecting 158,711 patient records. There may have been more incidents in which paper or film records were involved, but some reports were lacking to make that determination.



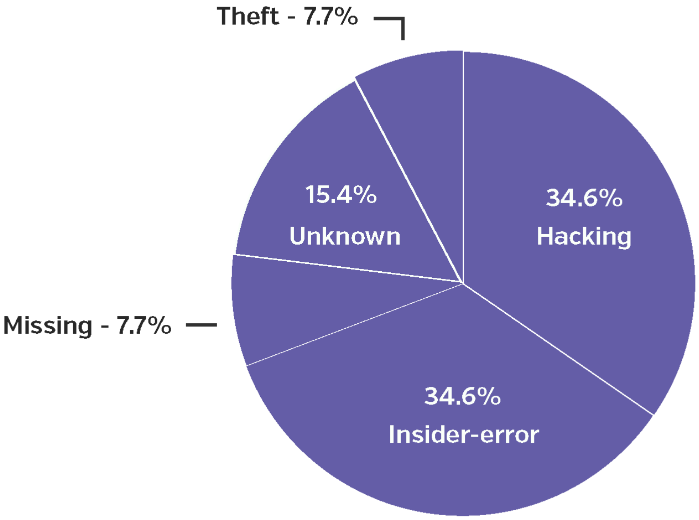
Types of entities disclosing, Q2 2018 health data breaches



Paper vs. electronic medical records in disclosed breaches, Q2 2018 health data breaches

Nearly 800,000 records breached as a result of business associate/third-party involvement

There were a total of 26 disclosed incidents that involved business associates (BAs) or third-party vendors (18.3% of total incidents). Information is available for 22 of these incidents, affecting 796,875 patient records (25.3% of total patient records). There were nine instances in which a business associate was involved with a hacking incident, nine insider-error incidents, two insider-wrongdoing incidents, two incidents of theft, and one incident 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.

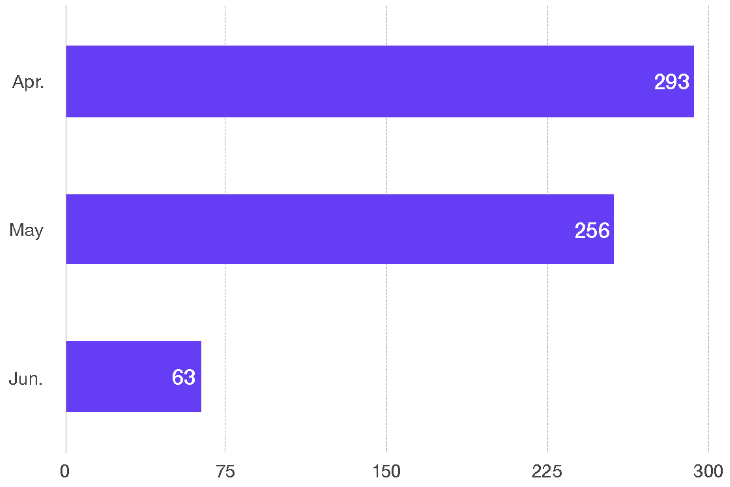


Business associate or third-party involvement in disclosed data breaches, Q2 2018 health data breaches

Insider-wrongdoing incident took 4+ years to discover

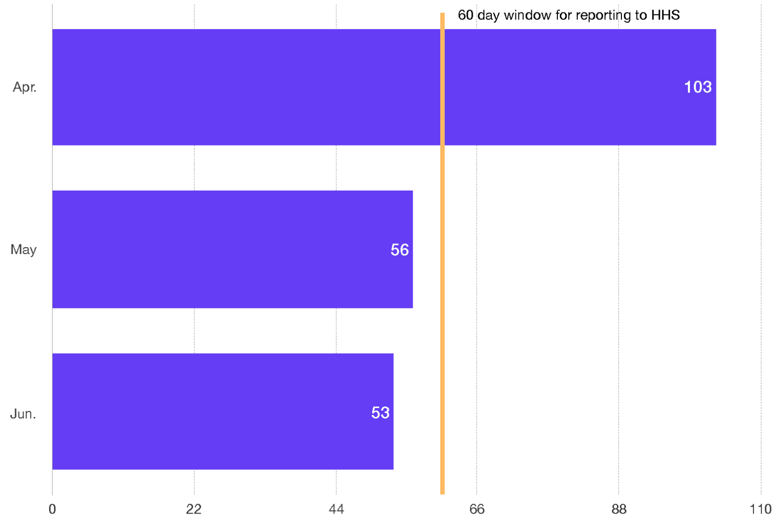
Of the 142 health data breaches for which data was disclosed, it took an average of 204 days from when the breach occurred to when it was discovered. The median discovery time was 18 days. There was a wide variety in the data, with the shortest discovery time of one day and the longest of 1,587 days (4.35 years).

The longest incident to be discovered in Q2 2018 was due to insider-wrongdoing at a California-based physician association. The incident occurred when a former employee took patient information before her employment ended, dating back to March 2013. The patient information included diagnoses, test results, medication, and other treatment information. The incident was finally discovered in March 2018, affecting 5,485 patient records.



Average number of days from disclosed breach to discovery, Q2 2018 health data breaches

Of the 61 incidents for which data was disclosed, it took an average 71 days from when a breach was discovered to when it was disclosed to HHS, the media or other sources. The median disclosure time was 59 days. It is important to note that information is available for less than half of the breaches disclosed from April to June 2018, making it difficult to draw conclusions from the available data.

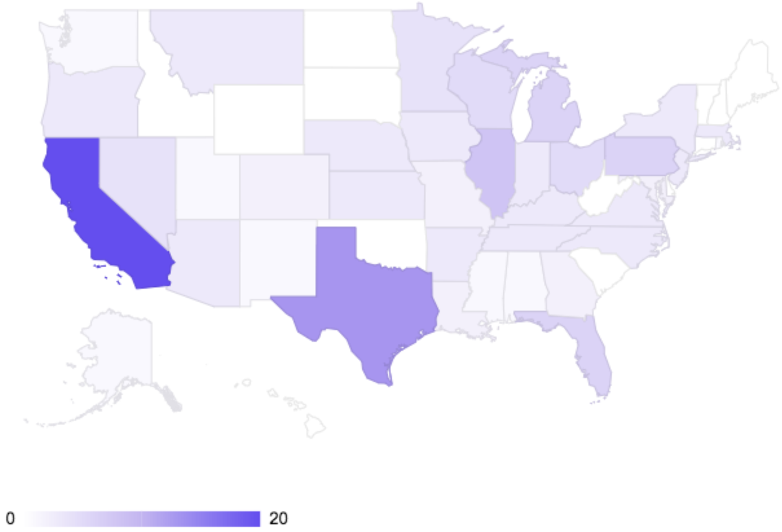


Average number of days from discovery to disclosure, Q2 2018 health data breaches

Insider incidents were associated with the longest gaps between the breach occurrence and detection. Generally, this is the case because insiders have legitimate access to the EHR, making it easier for inappropriate accesses to fall under the radar. As mentioned above, the longest breach reported so far in 2018 went on for over four years before it was discovered by the healthcare organization. This incident is not alone. Alarmingly, there was at least two other health data breaches this quarter that took over three years to be discovered, one of which was a confirmed result of insider-wrongdoing.

California and Texas have the most data breaches per state

38 states are represented in the 142 disclosed health data breaches for which we had location data between April and June 2018. California had, by far, the most data breaches of any state, with 20 separate incidents. Texas had the second highest rate, with 13 separate disclosed 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, Q2 2018 health data breaches

Conclusion

As patients continue to be anxious about the state of health data security, combined with a new study that found the average cost per breached record has increased 6.4% ($408 per record) over last year. Healthcare organizations must remain vigilant, looking for best practices in healthcare privacy that will allow them to audit every access to their patient data. Full visibility into how their data is being accessed and used will help organizations secure patient trust while preventing data breaches from having costly consequences for their organization.

About Protenus and Methodology

Protenus is a healthcare compliance analytics platform that uses artificial intelligence to audit every access to patient records for the nation's leading health systems. Protenus helps our partner hospitals make decisions about how to better protect their data, their patients, and their institutions. Health data breaches reported to the U.S. Department of Health and Human Services, or reported to the media, are just the tip of the iceberg. At scale, the data analyzed by the Protenus platform provides unprecedented insight into who is accessing patient data, and whether they are doing so appropriately. This de-identified, anonymized data provides the Protenus insights throughout this report.

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."