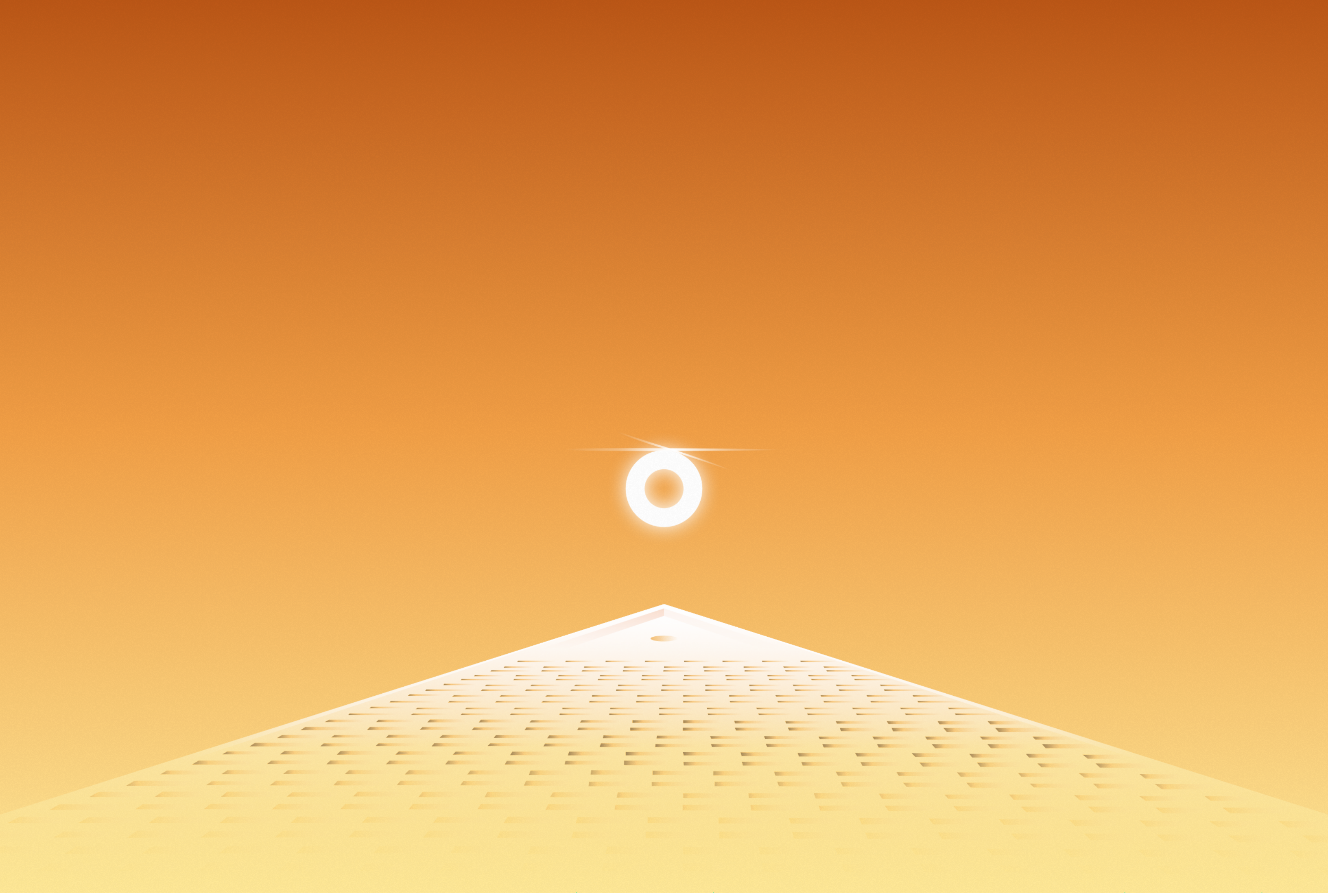


Q3 2018 PROTENUS BREACH BAROMETER

Insider-wrongdoing accounts for increasing number of breached patient records over the course of 2018

Protenus, Inc. in Collaboration with DataBreaches.net

PROTENUS

Breach Barometer Snapshot

July – September 2018

117 disclosed health data breaches

4.4M breached patient records

51.28% of total incidents were hacking

680K patient records breached by Insiders

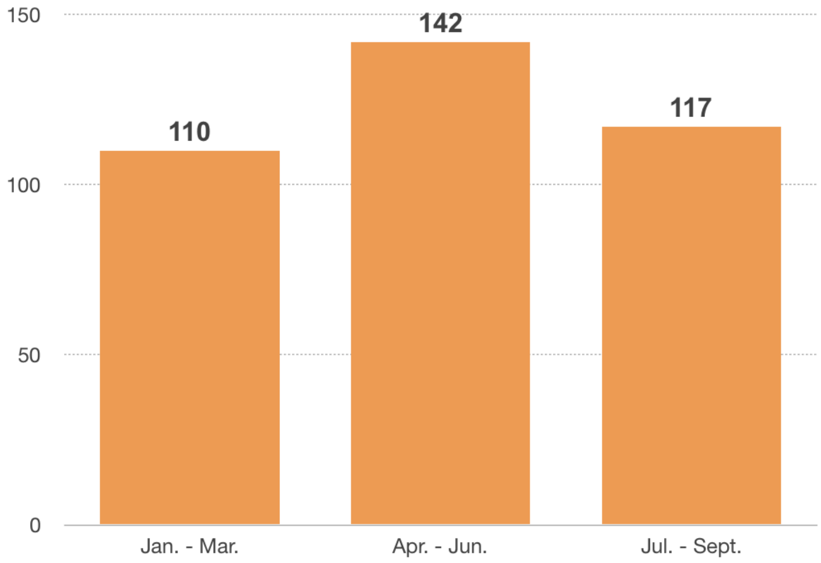
1.34M patient records breached by BA or third party

402 days, average time to discover a breach

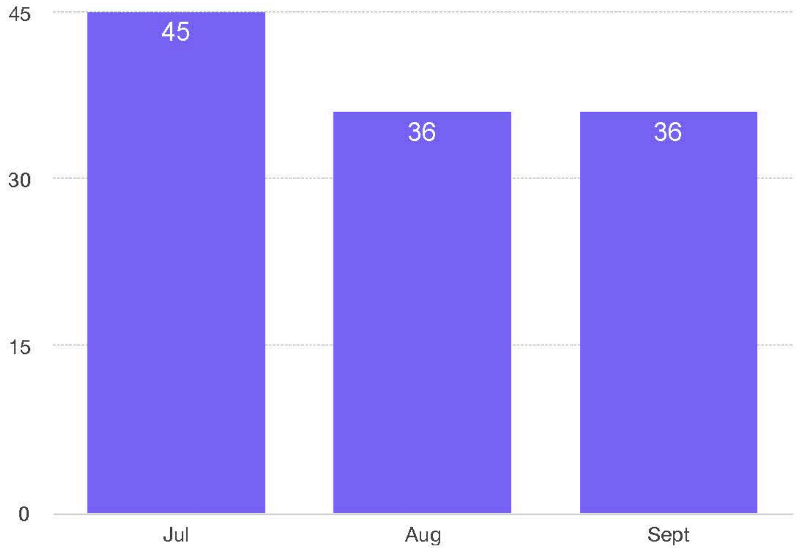
Florida had the most breaches with **11** incidents

Overview

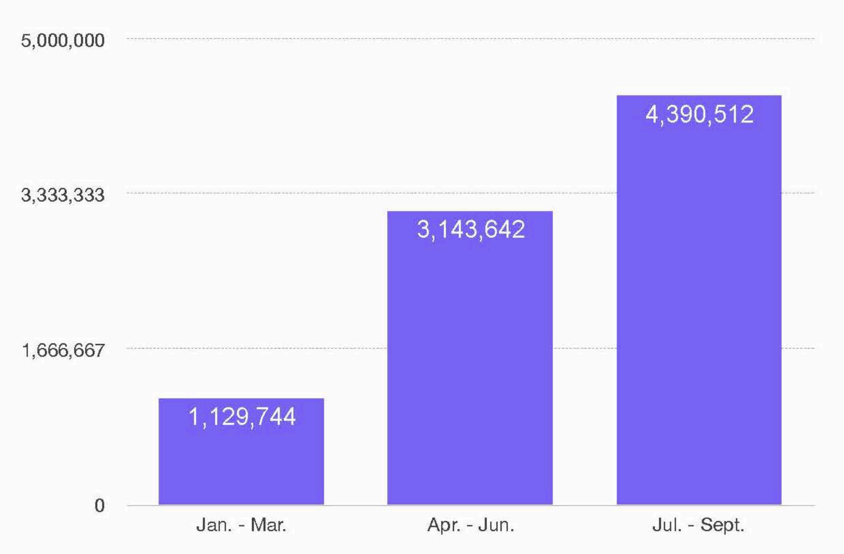
Health data security continues to be a significant challenge for the healthcare industry, with a total of 117 incidents disclosed to U.S. Department of Health and Human Services (HHS) or the media from July to September (Q3) 2018. Details were disclosed for 100 of these incidents, affecting 4,390,512 patient records. Although the number of incidents disclosed in Q3 decreased somewhat from Q2, the number of breached records increased from Q2 to Q3. It's important to note that the number of affected patient records has continued to climb each quarter in 2018, reinforcing the need for healthcare organizations to use advanced analytics and artificial intelligence to review 100% of accesses to patient data in order to prevent these breaches from occurring and to save organizations from post-breach costs that divert money from enhancing patient care.



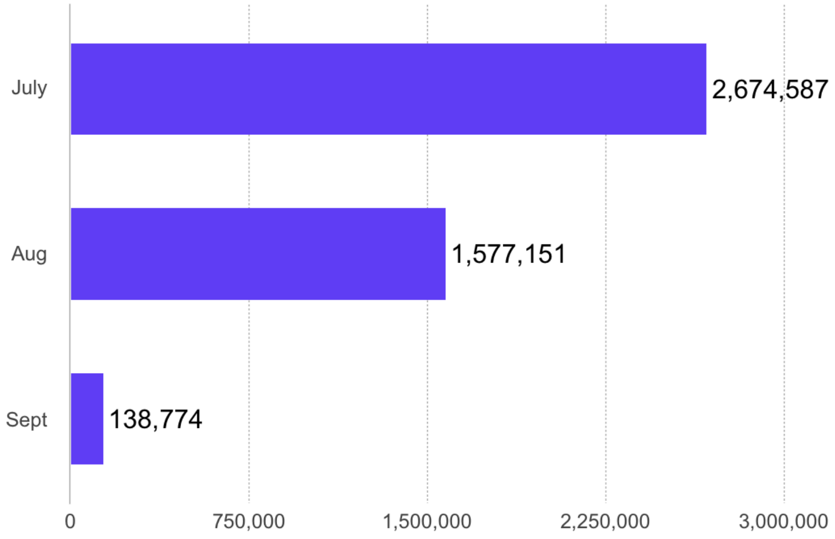
Quarterly comparison of total breach incidents, 2018 health data breaches



Number of breach incidents disclosed, Q3 2018 health data breaches

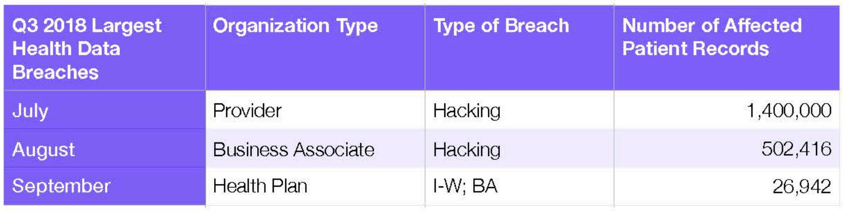


Quarterly comparison of breached patient records, 2018 health data breaches



Number of patient records in disclosed incidents, Q3 2018 health data breaches

The single largest breach in Q3 2018 was a hacking incident affecting 1.4M patient records that involved an Iowa-based health system. Hackers used phishing techniques - "official-looking emails" - to gain access to the organization's email system and capture employees' passwords. The hackers potentially gained access to patients' medical history, diagnoses, financial information, and types of care provided to the patient. This new incident follows one that took place at the same organization in April when 16,400 patient records were breached as a result of another phishing attack. Recurring phishing attacks are an unfortunate reminder of the vulnerabilities that many healthcare organizations face. However, technology now exists that will immediately detect when an employee's credentials are being misused, saving health systems from the devastating and costly effects of health data breaches like the ones mentioned above.



Q3 2018 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
July	Provider	Hacking	1,400,000
August	Business Associate	Hacking	502,416
September	Health Plan	I-W; BA	26,942

Largest disclosed incidents, Q3 2018 health data breaches

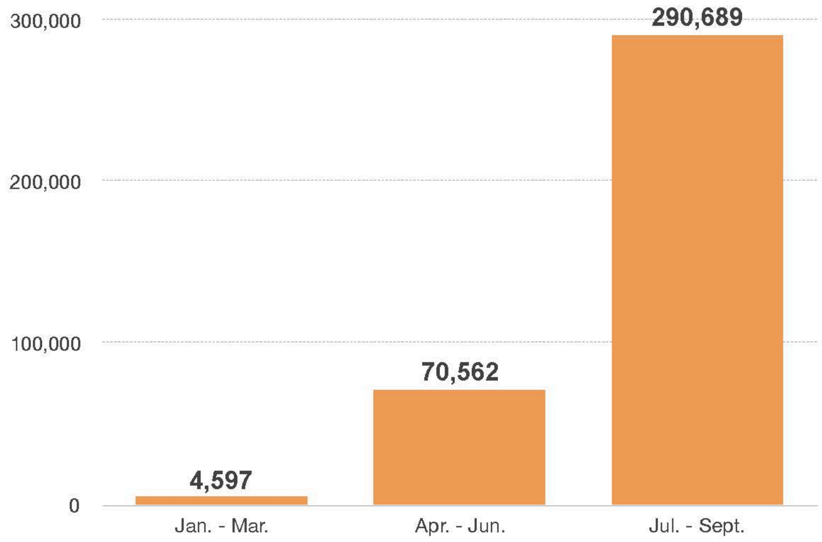
Insider-wrongdoing breaches increasingly more patient records each quarter in 2018

For incidents disclosed to HHS or the media, insiders were responsible for 23.08% of the total number of breaches in Q3 2018 (27 incidents). Details were disclosed for 21 of those incidents, affecting 680,117 patient records (15% of total breached patient records).

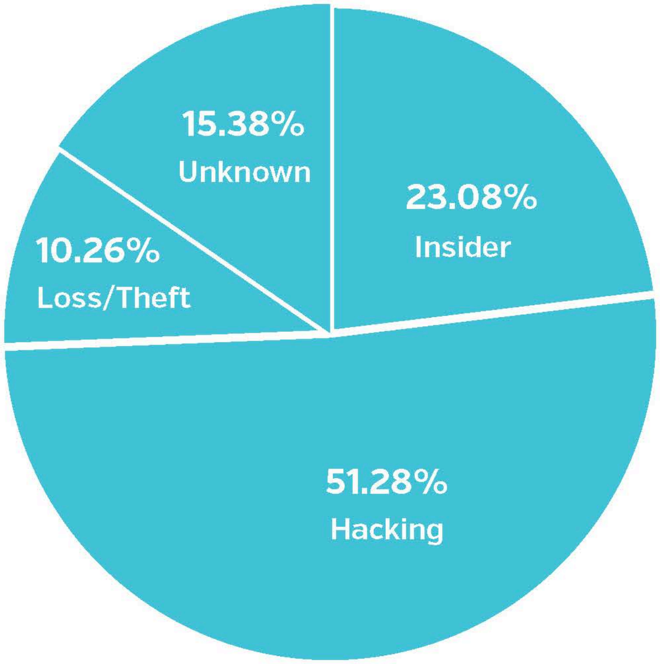
For the purposes of our analysis, insider incidents are characterized as either insider-error or insider-wrongdoing. The former includes accidents and other incidents without malicious intent that could be considered “human error.”

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 19 publicly disclosed incidents that involved insider-error between July and September 2018. Details were disclosed for 16 of these incidents, affecting 389,428 patient records. In contrast, eight incidents involved insider-wrongdoing, with data disclosed for five of these incidents. When comparing each quarter in 2018, there has been a drastic increase in the number of breached patient records as a result of insider-wrongdoing. In Q1 2018, there were only 4,597 affected patient records, in Q2 2018 there were 70,562 affected patient records, and in Q3 there were 290,689 affected patient records.



Patient records breached by Insider-wrongdoing (I-W), 2018 health data breaches



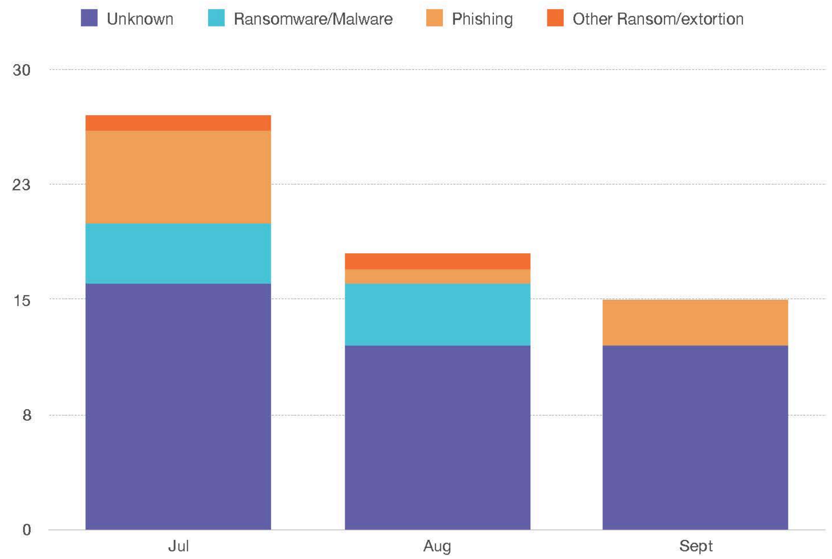
Type of disclosed incidents, Q3 2018 health data breaches

Hacking responsible for 83% of breached records between July and September

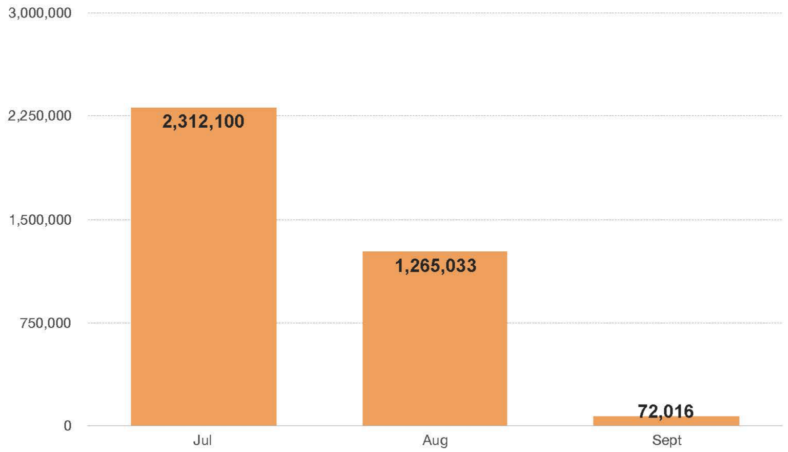
Hacking continues to threaten healthcare organizations, with another increase in incidents and affected patient records in the third quarter of 2018. Between July and September, there were 60 hacking incidents (51% of all Q3 2018 publicly disclosed incidents). Details were disclosed for 52 of those incidents, which affected 3,649,149 patient records. Eight of those reported incidents specifically mentioned ransomware or malware, ten incidents mentioned a phishing attack, and two incidents mentioned another form of ransomware or extortion. It's important to note that the number of incidents and affected patient records have dropped considerably when comparing each month between July and September 2018. Only time will tell if this trend continues, but the industry should monitor this data, as there could be seasonality to disclosed hacking incidents.

In addition to malware, ransomware, and phishing, there were ten reported incidents related to theft. Data was disclosed for eight of those incidents, which affected 24,328 patient records.

Finally, there were 18 disclosed incidents in which not enough information was available to categorize them, affecting 36,413 patient records.



Disclosed hacking incidents, Q3 2018 health data breaches

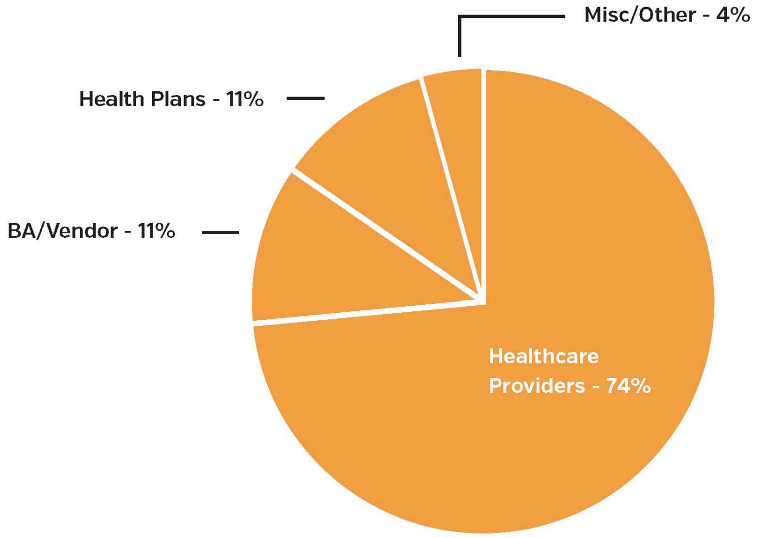


Patient records breached by disclosed hacking incidents, Q3 2018 health data

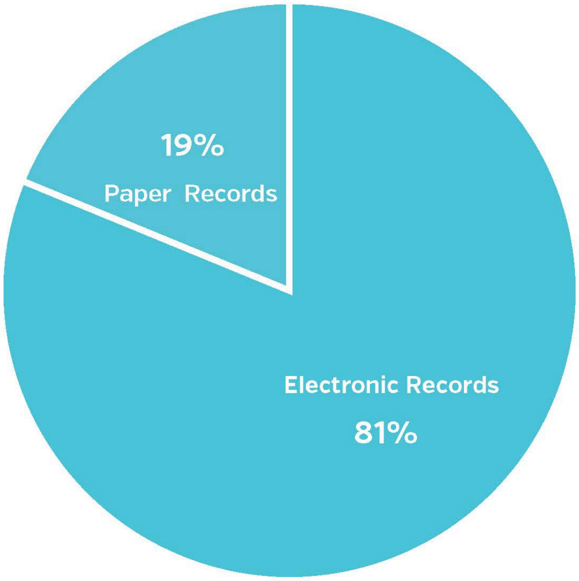
344K patient records affected by breached paper medical records

Of the 117 disclosed health data breaches that occurred between July and September of 2018, 86 of them (74% of total incidents) were disclosed by a healthcare provider, 13 were disclosed by a health plan, 13 were disclosed by a business associate or third-party vendor, and five were disclosed by businesses or other organizations.

Even though most healthcare organizations have already switched over to digitized patient records, 22 breach incidents still involved paper records. Disclosed data was available for 19 incidents, affecting 344,729 patient records. There may have been more incidents in which paper or film records were involved, but some reports were lacked sufficient information to make that determination.



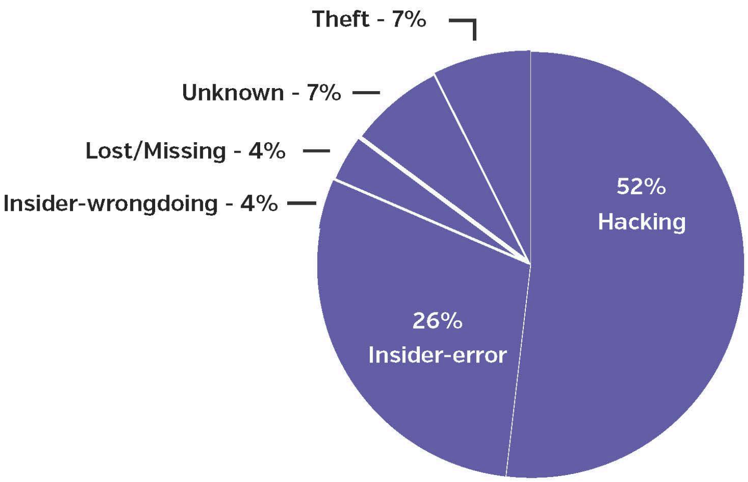
Type of entities disclosing, Q3 2018 health data breaches



Paper vs. electronic medical records in disclosed breaches, Q3 2018 health data breaches

Business Associates and vendors involved in 23% of breach incidents

There were a total of 27 disclosed incidents that involved business associates (BAs) or third-party vendors (23% of total incidents). Information is available for 23 of these incidents, affected 1,339,612 patient records (31% of total patient records). There were 14 instances in which a business associate was involved with a hacking incident, seven insider-error incidents, one insider-wrongdoing incident, two incidents of theft, and two 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.

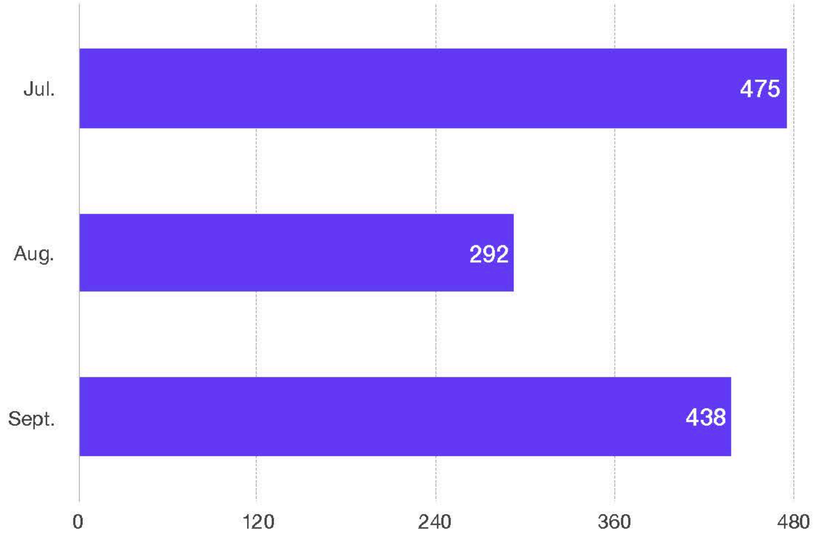


Business Associate or third-party involvement, Q3 2018 health data breaches

One insider-wrongdoing incident took 15 years to discover

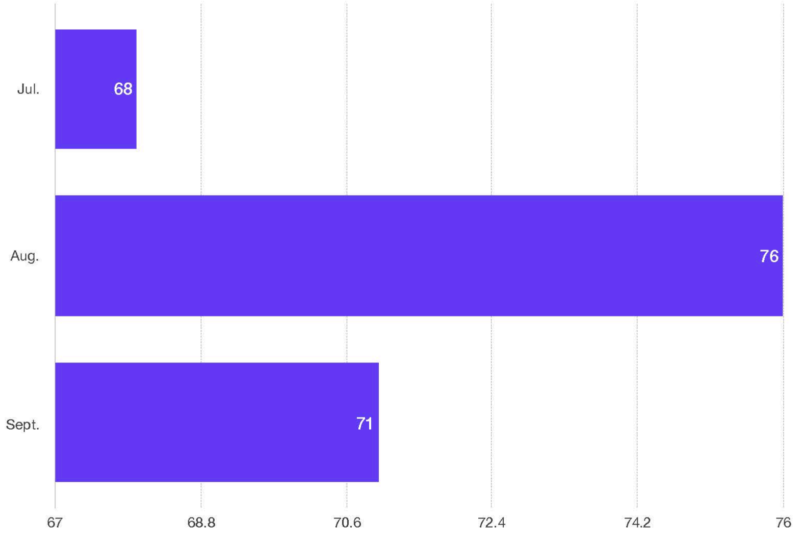
Of the 117 health data breaches for which data was disclosed, it took an average of 402 days to discover a breach from when the breach occurred. The median discovery time was 51 days. There were a wide variety of time frames for discovery, with the shortest discovery time of one day and the longest of 5,605 days (over 15 years).

The longest incident to be discovered in Q3 2018 was due to insider-wrongdoing at a Virginia-based healthcare organization. The incident occurred when an employee accessed thousands of medical records over the course of their 15-year employment. It is believed that this information was accessed without malicious intent. However, the employee has since been terminated. The patient information that was inappropriately accessed included addresses, dates of birth, medical record numbers, healthcare providers, visit date, health insurance information, and other sensitive information. The incident was finally discovered in July 2018, affecting 4,686 patient records.



Average number of days from breach to discovery, Q3 2018 health data breaches

Of the 53 incidents for which data was disclosed, it took an average of 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 57.5 days. It is important to note that information is available for less than half of the breaches disclosed from July to September 2018, making it difficult to draw conclusions from the available data.



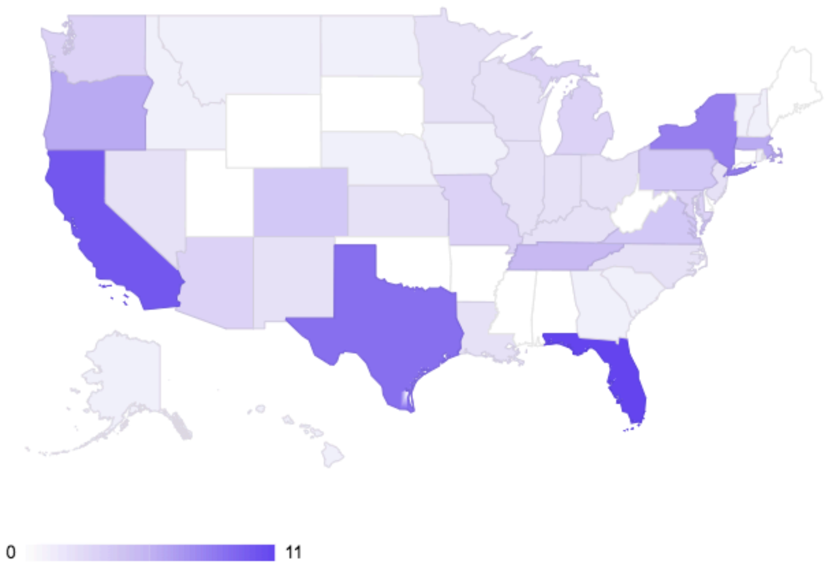
Average number of days from discovery to disclosure, Q3 2018 health data breaches

Insider incidents were associated with the longest gaps between breach occurrence and detection. Generally, this is the case because insiders have legitimate reasons to access the EHR, making it easier for inappropriate accesses to go under the radar. As mentioned above, the longest breach reported so far in 2018 went on for over fifteen years before it was discovered by the healthcare 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.

Florida has the most data breaches of any state

39 states are represented in the 117 disclosed health data breaches between July and September 2018 for which we had location data. Florida had the most data breaches of any state, with 11 separate incidents. California had the second highest number, with 10 separate disclosed incidents, followed closely

by Texas with nine 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, Q3 2018 health data breaches

Conclusion

There is an alarming trend that seems to be emerging with the sharp increase in patient records affected by insider-wrongdoing incidents each quarter so far in 2018. It's also possible that this trend is simply an artifact of better breach detection and reporting for incidents that would have previously gone undetected or undisclosed to the public. Regardless, in order for healthcare organizations to combat the challenges associated with health data security, it is critical for healthcare privacy offices to leverage technology 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 more sensitive information.

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."