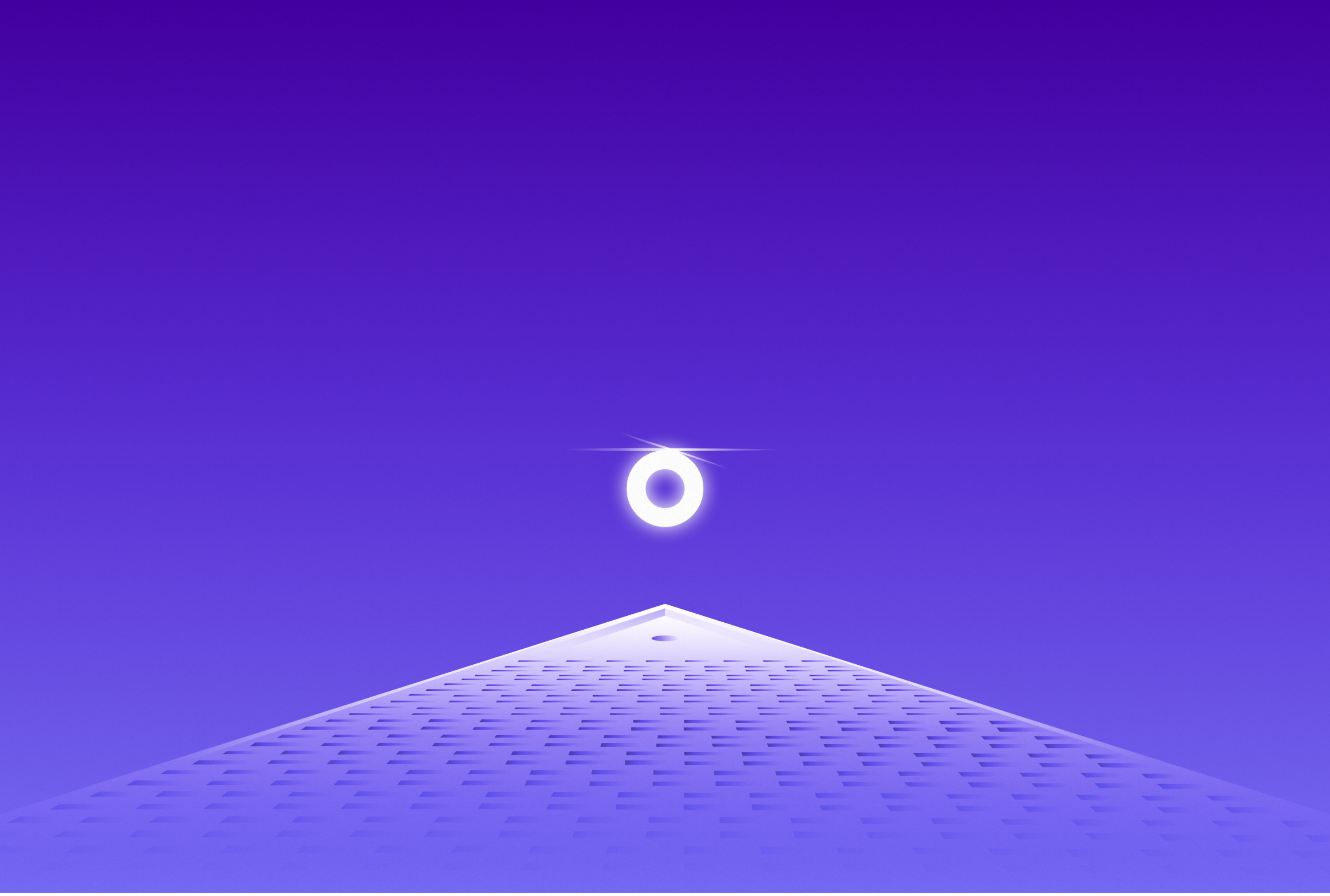


Q1 2018 PROTENUS BREACH BAROMETER

1.13M Patient Records Breached in Q1 2018, Proprietary Data Shows Disclosed Breaches Are Just the Tip of the Iceberg

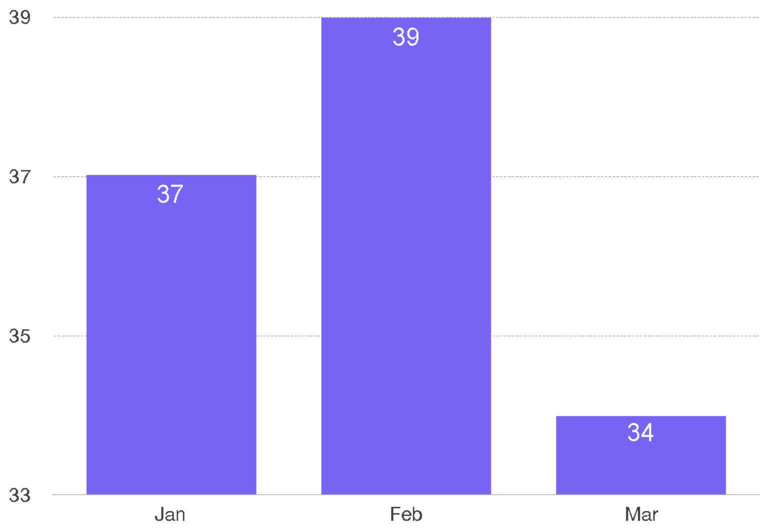
Protenus, Inc. in Collaboration with DataBreaches.net

Overview

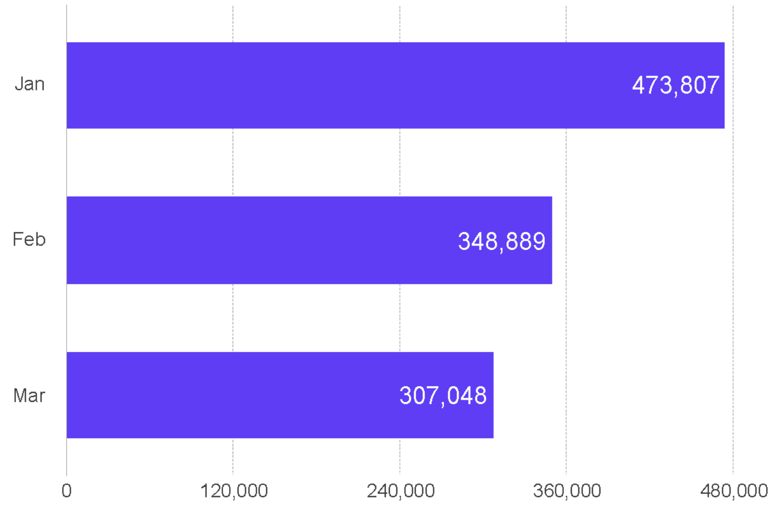
In Q1 2018, the trend of an average of at least one disclosed health data breach per day continues to hold true. There were a total of 110 health data breaches disclosed to U.S. Department of Health and Human Services (HHS) or the media from January to March (Q1) 2018. Details were disclosed for 84 of these incidents, affecting 1,129,744 patient records.

The single largest breach in Q1 2018 was a hacking incident that involved an Oklahoma-based healthcare organization, affecting 279,856 patient records. An unauthorized third-party gained access to the health system's network, which stored patient billing information, including patient names, Medicaid numbers, dates of service, and limited treatment information.

In addition to incidents disclosed to HHS or the media, this report compiles proprietary, non-public data on the status of health data breaches nationwide in Q1 2018. The analysis involved a review of tens of trillions individual accesses to electronic health records by Protenus, a healthcare compliance analytics platform used by hospitals to audit access to health data.



Number of breach incidents disclosed, Q1 2018 health data breaches



Number of affected patient records in disclosed incidents, Q1 2018 health data breaches

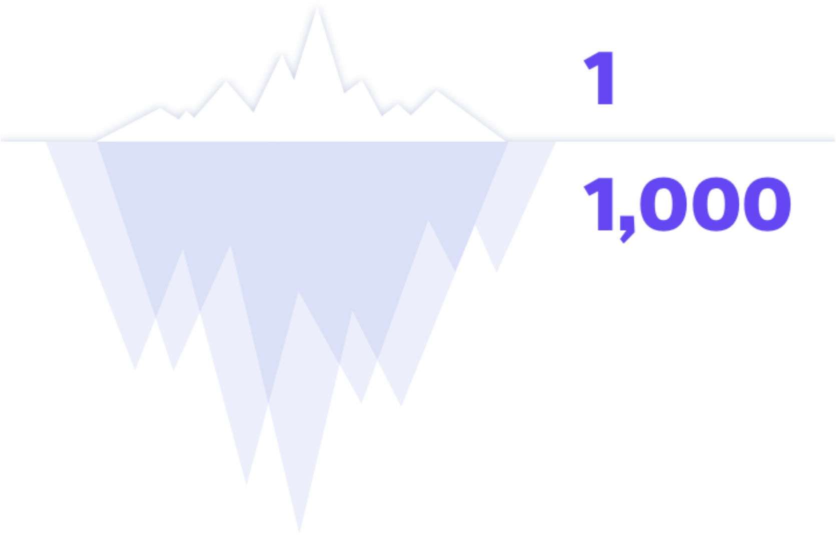
2018 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
January	Provider	Hacking	279,865
February	Provider	Hacking	135,000
March	Provider	Insider-error	63,551

Largest disclosed incidents, Q1 2018 health data breaches

Known breaches represent just the tip of the iceberg

The Kaiser Family Foundation estimates total healthcare employment at 12.4M individuals. Assuming that one insider incident represents one healthcare employee, publicly disclosed data suggest that roughly 1 in 300,000 healthcare employees have breached privacy in the first three months of 2018.

However, Protenus data suggest that as many as 1 in 300 healthcare workers have been involved in a privacy breach between January and March 2018. This means that reported violations only represent one one-thousandth of the actual risk health systems routinely carry.



Disclosed privacy violations vs. actual health system risk, Q1 2018 health data breaches

Family member snooping is the most common insider-related breach

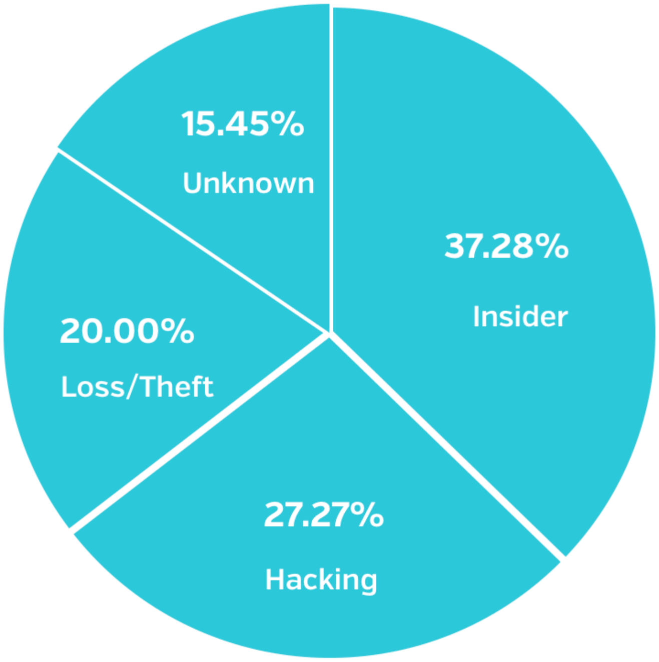
The largest category of health data breaches in Q1 2018 involved insiders, or healthcare organization employees with legitimate access to patient medical records. Protenus data discovered that on average, 3.38 healthcare employees breach patient privacy per every 1,000 employees.

For incidents disclosed to HHS or the media, insiders were responsible for 37.28% of the total number of breaches in Q1 2018 (41 incidents). Details were disclosed for 32 of those incidents, affecting 386,599 patient records (34% of total breached patient records).

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."

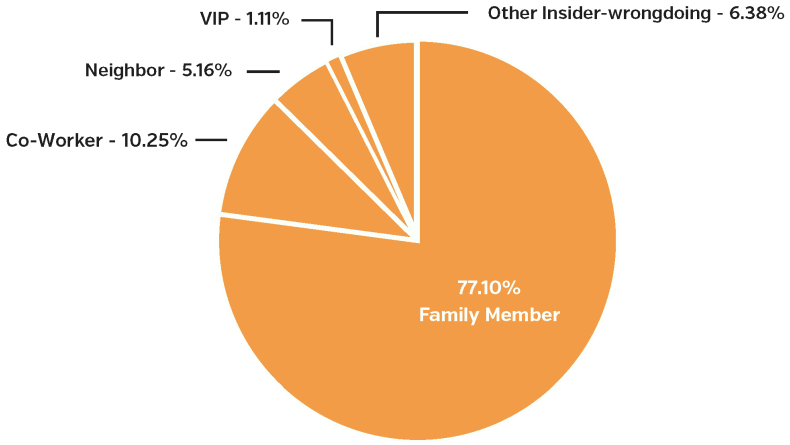
Insider-wrongdoing includes employee theft of information, snooping in patient files, and other cases where employees appeared to have knowingly violated the law.

There were 32 incidents publicly disclosed that involved insider-error between January and March 2018, and details were disclosed for 27 of them. In contrast, nine incidents involved insider-wrongdoing, with data disclosed for five of these incidents. Insider-error incidents affected 382,002 patient records and insider-wrongdoing affected 4,597 records.



Type of disclosed incidents, Q1 2018 health data breaches

Healthcare insiders were most likely to snoop on their family members (77.10% of violations) when breaching privacy. Snooping on fellow co-workers (10.25% of violations) was the second most common insider-wrongdoing violation, followed by snooping on neighbors (5.16%) and VIP-related (1.11%) incidents. The "other insider-wrongdoing" category included less common, but often more malicious, incidents like phishing attacks, insider credential sharing, downloading records for sale, identity theft, or other types of nefarious behaviors.

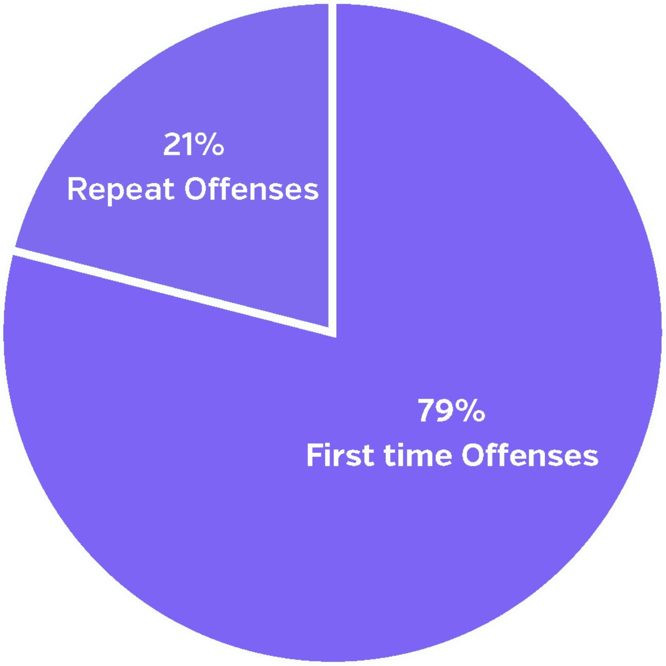


Insider incidents by category of violation, Q1 2018 health data breaches

Insiders are significantly more likely to breach privacy after first violation

If an individual healthcare employee breaches patient privacy once, there is a greater than 20% chance that they will do so again in three months' time, and a greater than 54% chance they will do so again in a years' time. In Q1 2018, 21% of privacy violations were repeat offenses. This evidence indicates health systems accumulate risk that compounds over time if proper reporting, education, and discipline actions do not occur.

Resources provided to healthcare organizations are pivotal in reducing the number of breach incidents that occur. Educating staff on EHR policy and procedures has been shown to reduce the frequency of repeat offenders within the organization.



First time vs. repeat offenses to patient privacy, Q1 2018 health data breaches

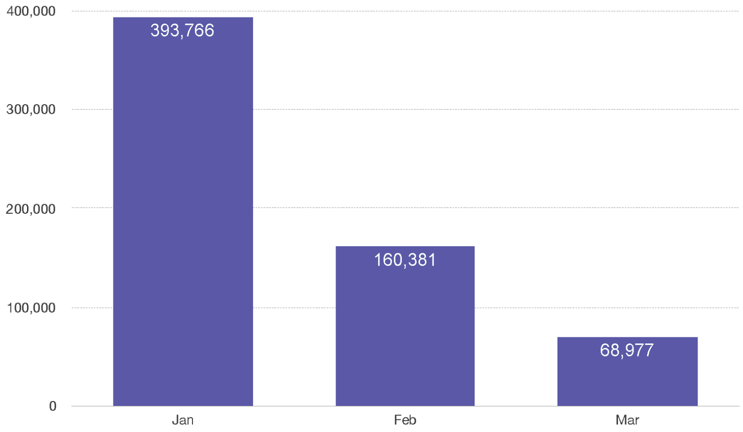
Hacking responsible for 55% of breached patient records in Q1 2018

Hacking has been a consistent threat to healthcare organizations in the first three months of 2018, with a total of 30 incidents (27.27% of all 2018 breaches). Details were disclosed for 19 of those incidents, which affected 623,124 patient records. 11 of those reported incidents specifically mentioned ransomware or malware and five incidents mentioned a phishing attack.

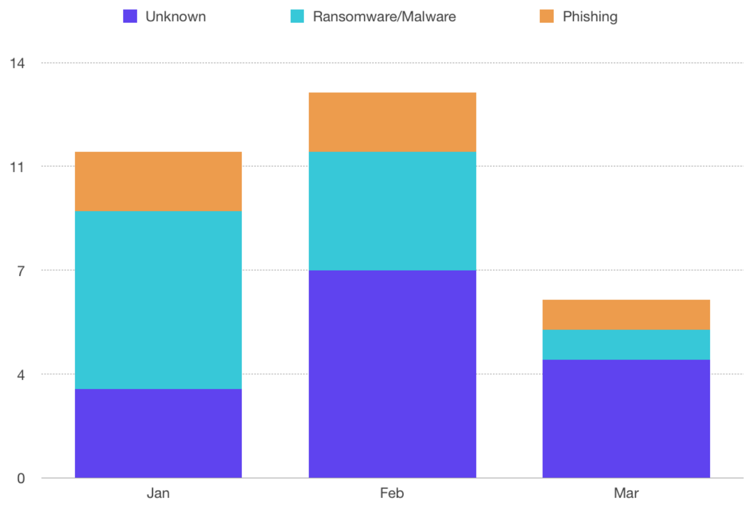
A survey published earlier this year found that the majority of information technology and security officials said that 'preventing malware and ransomware' was a top initiative for building a cyber resilience strategy over the next year. The survey also found that 78% of provider organizations have dealt with ransomware, malware, or both in the last 12 months, reinforcing the need for healthcare organizations to continue to make patient data security a top priority.

In addition to malware, ransomware, and phishing, there were 14 reported incidents related to theft. Data was disclosed for nine of those incidents, which affected 71,338 patient records. Eight incidents involved missing or lost records, affecting 17,001 patients records.

Finally, there were 17 disclosed incidents in which not enough information was available to categorize them. We have numbers for four such incidents, affecting 31,682 patient records.



Patient records breached by disclosed hacking incidents, Q1 2018 health data breaches

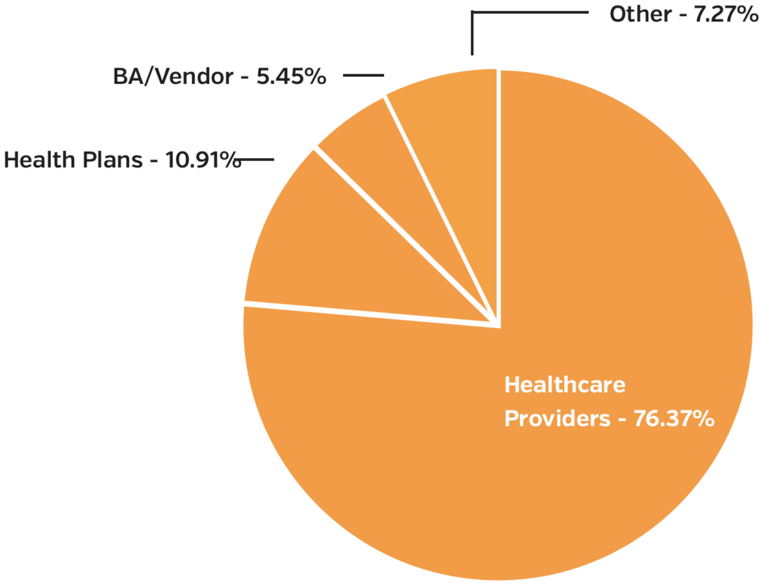


Disclosed hacking incidents, Q1 2018 health data breaches

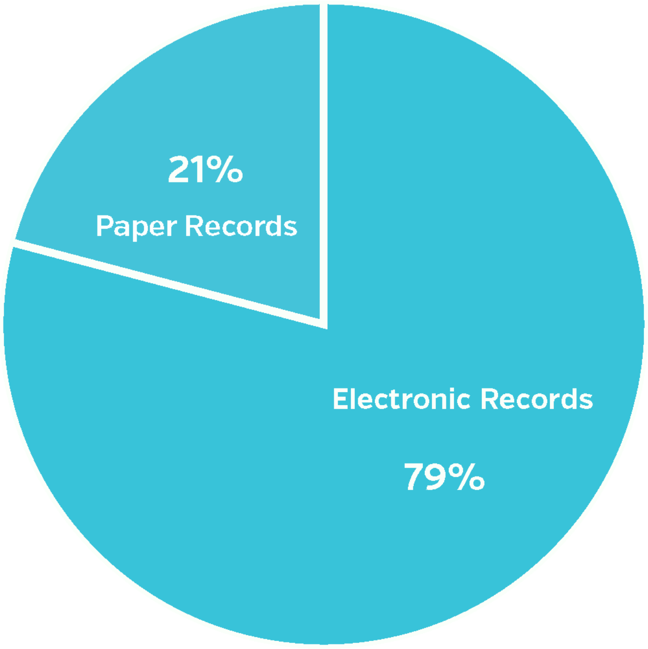
23 breach incidents still involved paper records

Of the 110 disclosed health data breaches that occurred between January and March of 2018, 84 of them (76.37% of total incidents) were disclosed by a healthcare provider, 12 were disclosed by a health plan, six were disclosed by a business associate or third-party vendor, and eight 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.



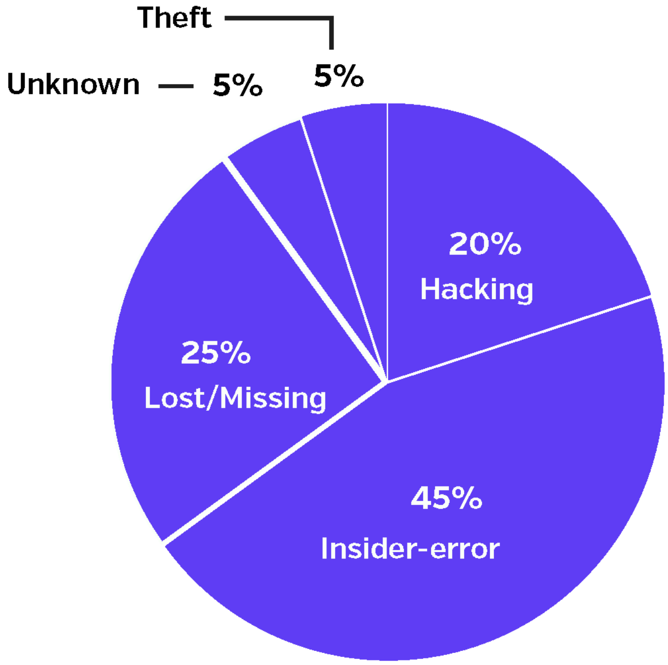
Types of entities disclosing, Q1 2018 health data breaches



Paper vs. electronic medical records in disclosed breaches, Q1 2018 health data breaches

Business associate/third-party involvement

There were a total of 20 disclosed incidents that involved business associates (BAs) or third-party vendors (18% of total incidents). Information is available for 14 of these incidents, affecting 180,865 patient records (16% of total patient records). There were four instances in which a business associate was associated with a hacking incident, nine insider-error incidents, one incident of theft, one uncategorized incident, and five incidents in which a BA was involved in patient records that were lost or missing. 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.

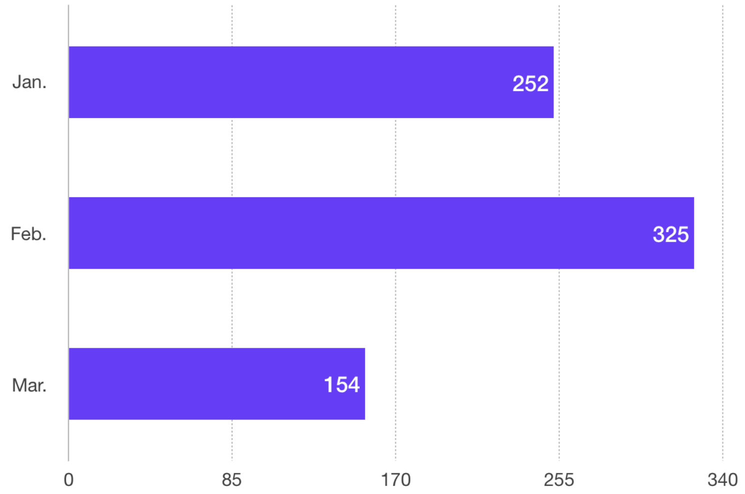


Business associate or third-party involvement in disclosed data breaches, Q1 2018 health data breaches

244 days, average time for health data breach detection

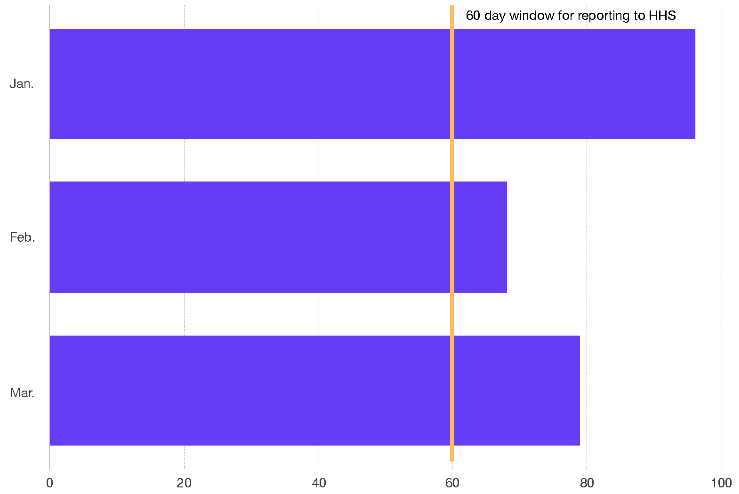
Of the 110 health data breaches for which data was disclosed, it took an average of 244 days from when the breach occurred to when it was discovered. The median discovery time was 23 days. There was a wide variety in the data, with the shortest discovery time of one day and the longest of 1,150 days (4.14 years).

One insider-error incident in Q1 2018 was caused by a business associate that took more than four years (1,510 days) to detect. The affected healthcare organization had taken over onsite clinics for three of its clients. In February 2017, that organization became aware that there was an issue with their health record system, and began an investigation. In December 2017, the healthcare organization found a technical issue allowing employees of their clients to access more information within the record system than those employees should have had been given access to. According to the organization's report to HHS, 4,549 patient records were affected.



Average number of days from disclosed breach to discovery, Q1 2018 health data breaches

Of the 56 incidents for which data was disclosed, it took an average of 81 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 there is only information available for approximately half of the breaches disclosed from January to March 2018, making it difficult to draw conclusions from the available data.



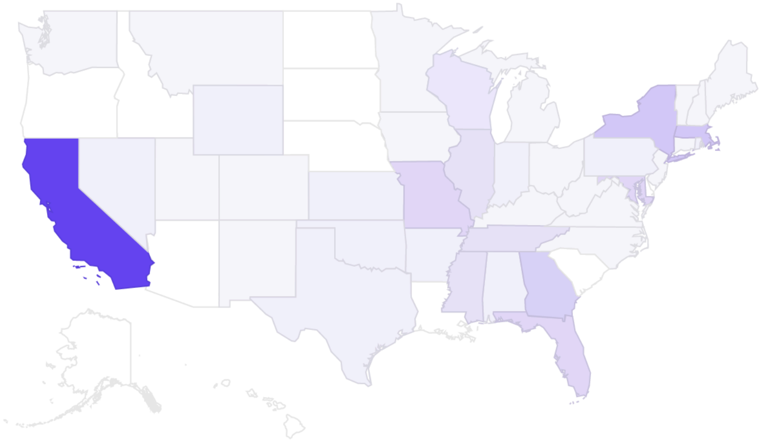
Average number of days from discovery to disclosure, Q1 2018 health data breaches

In general, healthcare entities are able to detect hacking incidents quicker than insider incidents, but incidents of hacking tended to have slightly longer gaps between the discovery of the breach and reporting it. This may be due, in part, to law enforcement officials asking organizations not to disclose the breach publicly as they continue their investigation.

Insider incidents were associated with the longest gaps between the breach occurrence and detection. This can be 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. And this incident is not alone. There was at least one other health data breach that took almost four years to be discovered.

California had the most breach incidents in Q1 2018

40 states and Washington D.C. are represented in the 110 disclosed health data breaches for which we had location data in Q1 2018. California had, by far, the most data breaches of any state, with 20 separate incidents. Massachusetts and New York had the second highest rate of breach incidents, with each state having suffered seven disclosed incidents. It is important to note that California often has more reported breaches, and this could be due to a higher number of reporting entities and patient volume, and/or more robust reporting methods and procedures.



Number of disclosed incidents by state, Q1 2018 health data breaches

It is also important to note that South Dakota and Alabama recently passed breach laws. This is critical, as now all fifty states have passed laws to better protect sensitive personally identifiable information. Oregon has also amended current state breach laws to expand the scope of covered individuals and update prescriptive security measures. Maryland and Colorado have also proposed amendments to current laws, Maryland wanting to require Internet Service Providers (ISP) to notify customers when there is a breach, and Colorado wanting to create stricter data breach reporting requirements.

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."