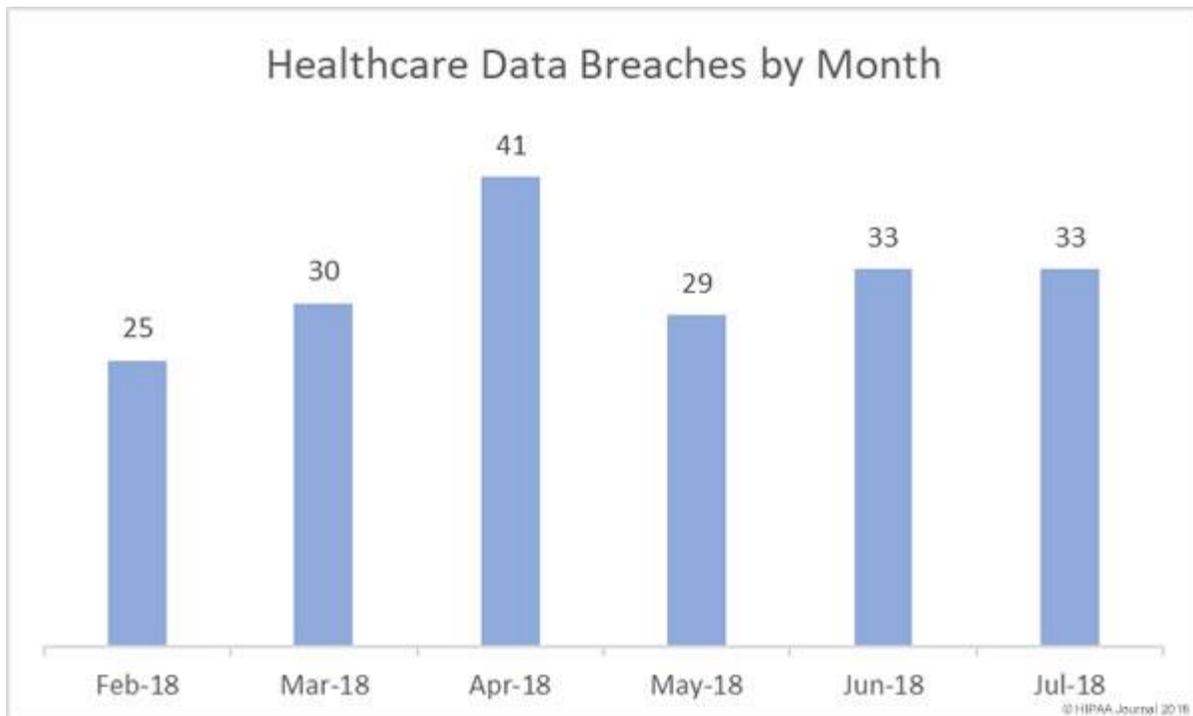


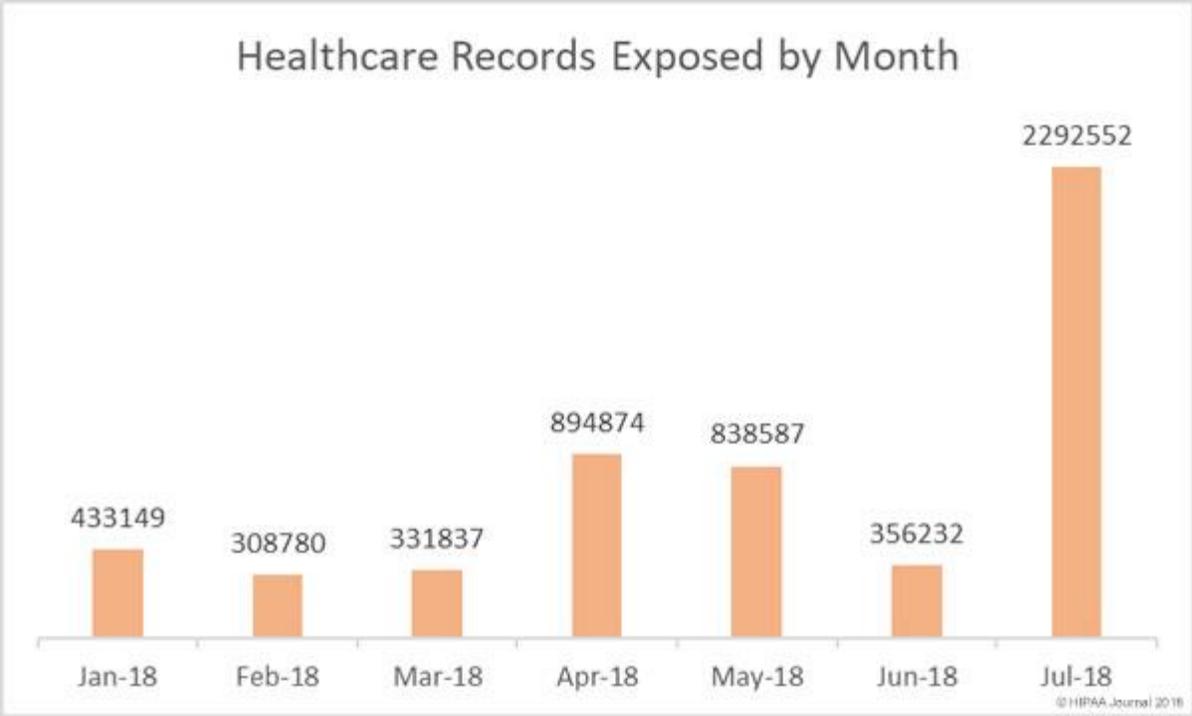
## July 2018 Healthcare Data Breach Report

HIPAA Journal  
August 24, 2018

July 2018 was the worst month of 2018 for healthcare data breaches by a considerable distance. There were 33 breaches reported in July – the same number of breaches as in June – although 543.6% more records were exposed in July than the previous month.



The breaches reported in July 2018 impacted 2,292,552 patients and health plan members, which is 202,859 more records than were exposed in April, May, and June combined.



**A Bad Year for Patient Privacy**

So far in 2018 there have been 221 data breaches of more than 500 records reported to the Department of Health and Human Services’ Office for Civil Rights. Those breaches have resulted in the protected health information of 6,112,867 individuals being exposed, stolen, or impermissibly disclosed. To put that figure into perspective, it is 974,688 more records than were exposed in healthcare data breaches in all of 2017 and there are still five months left of 2018.

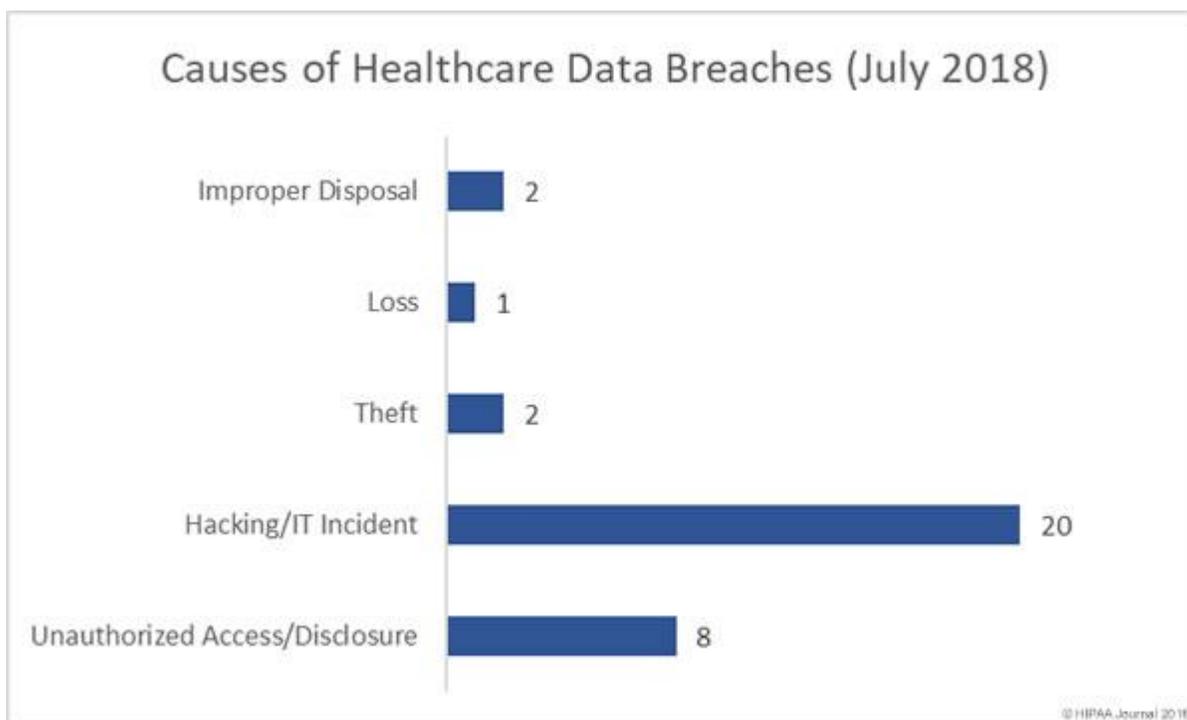
**Largest Healthcare Data Breaches of 2018 (Jan-July)**

Entity Name	Entity Type	Records Exposed	Breach Type
UnityPoint Health	Business Associate	1,421,107	Hacking/IT Incident
CA Department of Developmental Services	Health Plan	582,174	Theft
MSK Group	Healthcare Provider	566,236	Hacking/IT Incident
LifeBridge Health, Inc	Healthcare Provider	538,127	Hacking/IT Incident
SSM Health St. Mary’s	Healthcare Provider	301,000	Improper Disposal

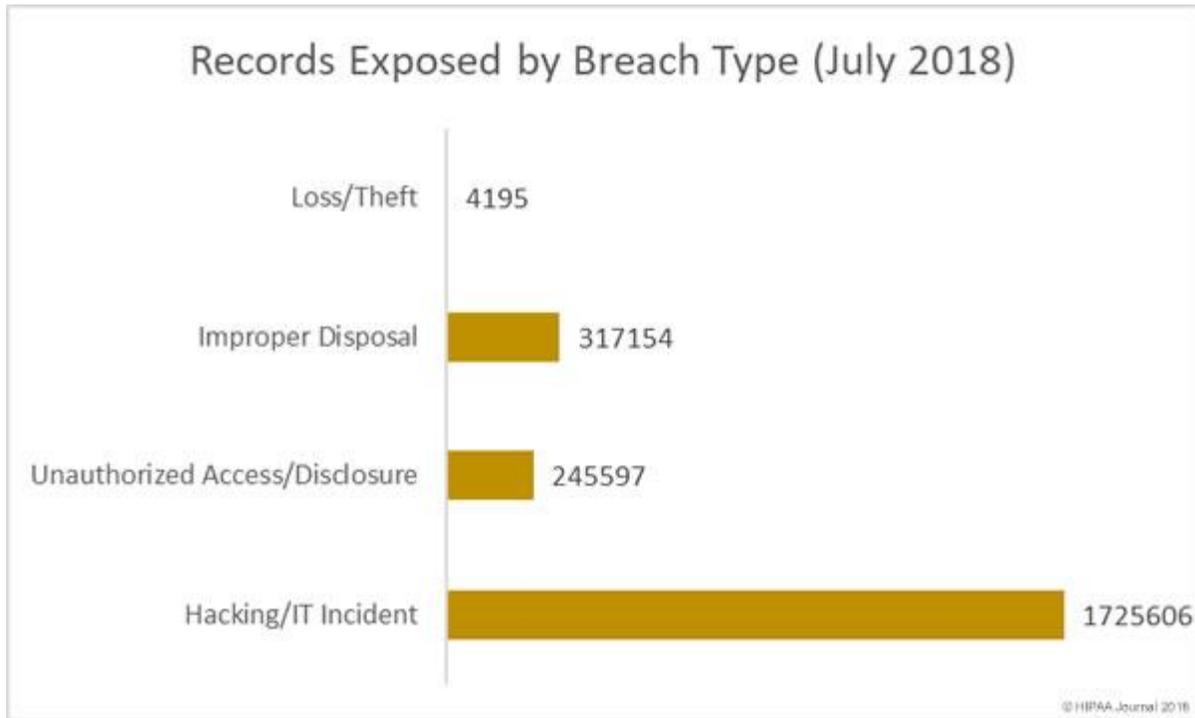
Hospital – Jefferson City			
Oklahoma State University Center for Health Sciences	Healthcare Provider	279,865	Hacking/IT Incident
Med Associates, Inc.	Business Associate	276,057	Hacking/IT Incident
MedEvolve	Business Associate	205,434	Unauthorized Access/Disclosure
St. Peter’s Surgery & Endoscopy Center	Healthcare Provider	134,512	Hacking/IT Incident
Boys Town National Research Hospital	Healthcare Provider	105,309	Hacking/IT Incident

### Causes of Healthcare Data Breaches in July 2018

Unauthorized accessing of PHI by employees and impermissible disclosures of PHI are commonplace in healthcare, although in July there was a major reduction in these types of breaches, falling by 46.6% from July. There was also a significant drop in the number of incidents involving the loss or theft of unencrypted electronic devices and physical PHI, which fell 50% month over month.



Hacking incidents, ransomware attacks and other IT incidents such as malware infections and phishing attacks significantly increased in July. There were 66.7% more hacking/IT incidents than June. Hacking/IT incidents also resulted in the exposure of more healthcare records than all other types of breaches combined.



7 of the 15 largest data breaches (46.7%) in July were phishing attacks, two were ransomware attacks, three were failures to secure electronic PHI and two were improper disposal incidents involving physical PHI. The improper disposal incidents were the second biggest cause of exposed PHI, largely due to the 301,000-record [breach at SSM Health](#). In that breach, physical records were left behind when St. Mary's Hospital moved to a new location.

In July, more healthcare records were exposed through phishing attacks than any other breach cause. The phishing incidents resulted in the exposure and possible theft of than 1.6 million healthcare records.

#### **Largest Healthcare Data Breaches in July 2018**

In July, there were 12 healthcare data breaches of more than 10,000 records and four breaches impacted more than 100,000 individuals. There were 14 breaches of between 1,000 and 9,999 records and 7 breaches of between 500 and 999 records. Four of the ten largest healthcare data breaches of 2018 were reported in July.

The largest healthcare data breach of July, and the largest breach of 2018 to date, was a phishing attack on Iowa Health System doing business as UnityPoint Health.

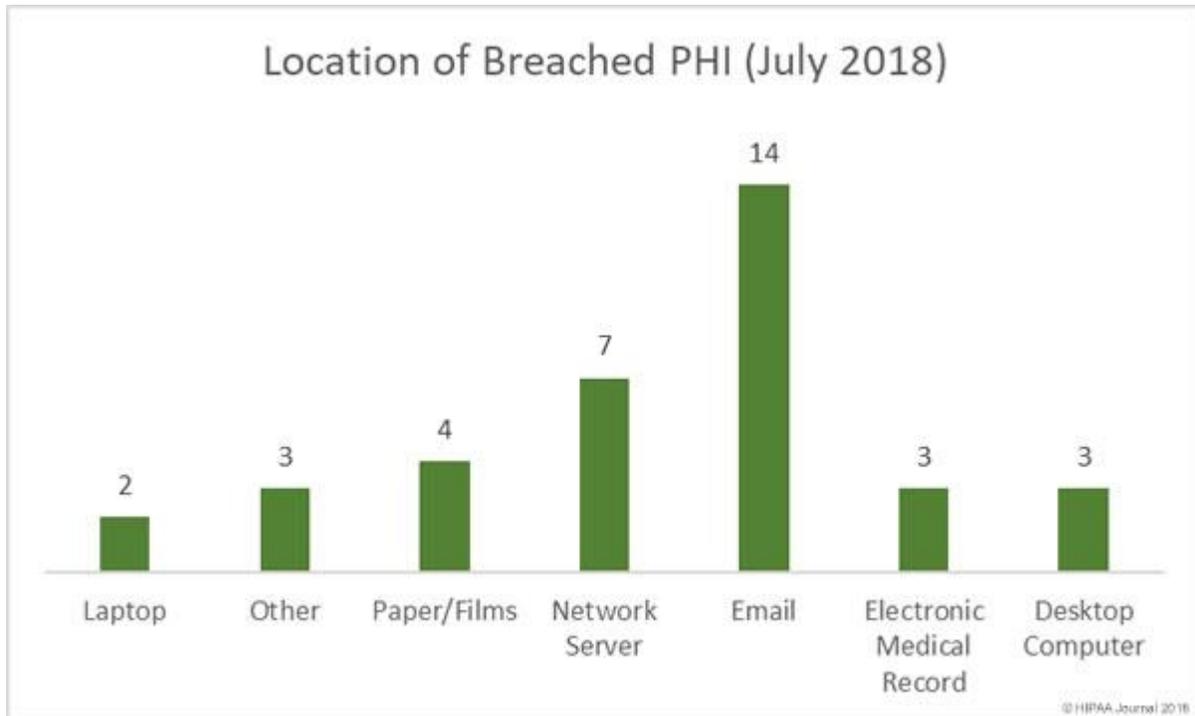
The threat actor responsible for the [UnityPoint Health phishing attack](#) spoofed an executive’s email account and sent messages to UnityPoint Health employees. Several members of staff were fooled by the emails and disclosed their login credentials giving the attacker access to their email accounts. Those email accounts contained the protected health information of more than 1.4 million patients.

Four of the ten largest healthcare data breaches of 2018 were reported in July.

<b>Entity Name</b>	<b>Entity Type</b>	<b>Records Exposed</b>	<b>Breach Type</b>
UnityPoint Health	Business Associate	1,421,107	Hacking/IT Incident
SSM Health St. Mary’s Hospital – Jefferson City	Healthcare Provider	301,000	Improper Disposal
MedEvolve	Business Associate	205,434	Unauthorized Access/Disclosure
Boys Town National Research Hospital	Healthcare Provider	105,309	Hacking/IT Incident
Blue Springs Family Care, P.C.	Healthcare Provider	44,979	Hacking/IT Incident
Golden Heart Administrative Professionals	Business Associate	44,600	Hacking/IT Incident
Confluence Health	Healthcare Provider	33,821	Hacking/IT Incident
NorthStar Anesthesia	Healthcare Provider	19,807	Hacking/IT Incident
Orlando Orthopaedic Center	Healthcare Provider	19,101	Unauthorized Access/Disclosure
New England Dermatology, P.C.	Healthcare Provider	16,154	Improper Disposal
MedSpring of Texas, PA	Healthcare Provider	13,034	Hacking/IT Incident
Longwood Orthopedic Associates, Inc.	Healthcare Provider	10,000	Unauthorized Access/Disclosure

### Location of Breached PHI

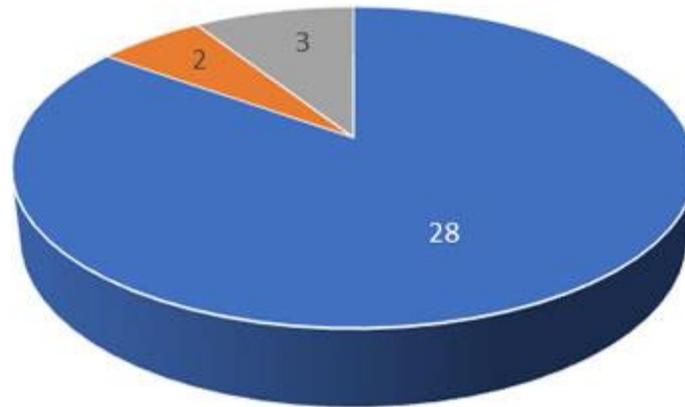
Unsurprisingly, given the high number of successful phishing attacks in July, email-related breached dominated the breach reports and was the main location of breached PHI, as has been the case in March, April, May and June. There were seven network server breaches in July, which were a combination of ransomware attacks, accidental removal of security protections, malware infections, and hacking incidents.



### Data Breaches by Covered Entity Type

Healthcare providers were hit the hardest in July with 28 breaches reported by providers. Only two health plans reported data breaches in July. Three business associates reported breaches, although nine reported data breaches had at least some business associate involvement.

## Data Breaches by Covered Entity (July 2018)



■ Healthcare Provider ■ Health Plan ■ Business Associate

© HIPAA Journal 2018

### Healthcare Data Breaches by State

Healthcare organizations based in 22 states reported data breaches in July. California usually tops the list for the most data breaches each month due to the number of healthcare organizations based in the state, although in July it was Florida and Massachusetts that had the most breaches with three apiece. Alaska, Missouri, New York, Pennsylvania, Texas, Virginia, and Washington each had two breaches reported, and there was one breach reported in each of Arkansas, California, Colorado, Idaho, Indiana, Illinois, Maryland, Michigan, Montana, Nebraska, New Jersey, New Mexico, and Tennessee.