CASE EVALUATION

HIPAA Security Violation Examples 2015-2017

Abstract

HIPAA Security violations pose a serious threat to healthcare organizations in the US. Between the years 2015 through 2017 to date, there have been, according to the US Department of Health and Human Services, 2,974,545 violations reported in the state of Florida. This report will examine: Unauthorized access/Disclosure; Hacking/IT Incident, and Theft - and will look at commonalities, differences, and visible trends among the cases examined. This report will only present cases from the state of Florida because this facility is solely in the state of Florida.

Sherwin L. Kendall

Name of Covered Entity	Covered Entity Type	Type of Breach	Location of Breached Information	Breach Submission Date	Breach Summaries
Sacred Heart Health System, Inc.	Healthcare Provider	Hacking/IT Incident	Email	3/16/2015	1
Mount Sinai Medical Center	Healthcare Provider	Unauthorized Access/Disclosure	Paper/Films	3/20/2015	2
Pediatric Gastroenterology, Hepatology & Nutrition of Florida, P.A.	Healthcare Provider	Theft	Paper/Films	8/24/2015	3
Tallahassee Memorial HealthCare, Inc.	Healthcare Provider	Hacker/IT Incident	Other	5/20/2016	4
Florida Department of Health	Healthcare Provider	Unauthorized Access/Disclosure	Paper/Films	4/13/2016	5
Lake Pulmonary Critical Care, PA	Healthcare Provider	Theft	Paper/Films	4/20/2016	6
Hillsborough County Aging Services Department	Healthcare Provider	Loss	Paper/Films	2/16/2017	7
WellCare Health Plans, Inc.	Healthcare Provider	Hacking/IT Incident	Network Server	2/9/2017	8
Nova Southeastern University	Healthcare Provider	Theft	Portable Electronic Device	5/2/2017	9

What do these cases have in common?

The cases in this evaluation all have one thing in common; they represent breaches which took place in the state of Florida, and which were all reported by healthcare providers. All but two of the cases used here involved employees or former employees who were perpetrators in these breaches.

What are their differences?

The cases differ in the types of breaches that occur amongst them; there are hacking/IT incidents; unauthorized data access and disclosures; theft and loss. The cases also varied in their severity relative to the number of affected individuals – 14,177 for Sacred Heart Health System, Inc.; 13,000 at Pediatric Gastroenterology, Hepatology & Nutrition of Florida, P.A. - Tallahassee Memorial HealthCare, Inc. affected 505 individuals.

Is there a trend in types, size, or location of breaches across the years? Explain this trend or lack of trend.

The data gathered suggests that the bulk of breaches took place at healthcare providers of varying organizational sizes; the data also suggests that are heavy incidents of breaches involving paper files. Although the data I've examined is specifically from the state of Florida; the overall data shows that the most breaches occurred in the most populous states in the US; California, Texas and Florida – with breach numbers 85, 61 and 51 respectively.

What were your impressions of the types of cases you read and their resolutions?

I was surprised to find out that so many healthcare providers have been, and are being targeted – however, given the rich amount of data that resides within these organizations this is understandable. I was also surprised to learn that a website exists that chronicles and publicly displays this information. I thought that the resolutions met when breaches occurred were reasonable within the context of the breaches themselves.

What are some of the lessons learned in these cases? Is there a theme?

I learned that healthcare organizations need to direct more efforts towards safeguarding the data entrusted to them. I also learned that greater emphasis should be given to the segmentation of data access by employees since the data here seems to suggest that a great deal of breaches occur at the hands of employees. The theme running through all of the cases I examined is that healthcare organizations seem to be lacking the necessary tools, personnel and protocols which could possibly reduce the amount and the magnitude of the breaches reported here.

Breach Summaries

1. Sacred Heart Health System, Inc.'s business associate (BA), St. Vincent Health, Inc., a third-party billing vendor, was subject to an email phishing attack resulting in the exposure of protected health information for 14,177 individuals.

2. The covered entity (CE), Mt. Sinai, discovered that an employee was printing paper face sheets in excess of her job duties for an illicit purpose. The face sheets contained the demographic and clinical information of 1,406 individuals.

3. An employee of the CE removed appointment sheets containing the names, social security numbers, dates of birth, and account numbers of 13,000 patients from the premises without authorization.

4. Tallahassee Memorial HealthCare, Inc., the covered entity (CE), discovered that an employee attempted to upload protected health information (PHI) containing patients' names, insurance numbers, payor financial information numbers, and account numbers to an unauthorized website.

5. The covered entity (CE), Florida Department of Health, discovered on February 17, 2016, that an additional 1,076 individuals were affected by a breach previously reported in 2013 as affecting 877 individuals. The breach occurred when an employee with legitimate access to PHI stole demographic information for illegal purposes

6. The covered entity (CE), Lake Pulmonary Critical Care, PA, discovered that a former employee removed patient medical records from the office and took them home.

7. A former employee found and returned a box of paper records containing protected health information (PHI) that had been missing for over five years and that belonged to the covered entity (CE), Hillsborough County Aging Services Department.

8. WellCare Health Plans has announced that 24,809 of its members have also been impacted by a security incident.

9. NSU learned that two encrypted portable hard drives were stolen from an NSU employee.

References

HIPAA Journal
(n.d.). Retrieved from http://www.hipaajournal.com/wellcare-health-reports-security-breach-affecting-24800-patients-8680/

NSU Newsroom
(n.d.). Retrieved from https://nsunews.nova.edu/nova-southeastern-university-issues-letters-to-patients-regarding-stolen-hard-drives-with-institute-for-neuro-immune-medicine-lab-results/

US Department of Health and Human Services Breach Portal
(n.d.). Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf