

TOP 5 HEALTH DATA BREACHES

(REPORTED SINCE SEPTEMBER 2009 ENACTMENT OF HIPAA BREACH NOTIFICATION RULE)

Recent news that Community Health Systems suffered a breach by a purported “advanced persistent threat group originating from China” illustrates yet again the healthcare sector’s vulnerability. Here’s a look at the sector’s top five data breaches:

OVER 17 MILLION PEOPLE AFFECTED

“The healthcare sector’s security and privacy controls differ from more secure industries ... and healthcare organizations may be easier targets.”

- Ann Patterson, Medical Identity Fraud Alliance



4.9



MILLION

PEOPLE AFFECTED

DATE: SEPTEMBER 2011

HERE’S WHAT HAPPENED

Backup tapes for the military health program were stolen from an SAIC employee’s car. The employee was responsible for transporting the tapes between federal facilities.

INFORMATION COMPROMISED

Social Security numbers, names, addresses, phone numbers, clinical notes, lab tests, prescriptions

BUSINESS ASSOCIATE INVOLVED

Science Applications International Corp.



4.5



MILLION

PEOPLE AFFECTED

DATE: APRIL AND JUNE 2014

HERE’S WHAT HAPPENED

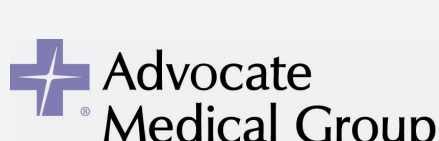
Hackers believed to be an “advanced persistent threat group originating from China” used malware to attack the hospital chain’s systems.

INFORMATION COMPROMISED

Names, addresses, birthdates, telephone numbers, Social Security numbers

BUSINESS ASSOCIATE INVOLVED

None



4.03



MILLION

PEOPLE AFFECTED

DATE: JULY 2013

HERE’S WHAT HAPPENED

Four unencrypted computers were stolen from the office of the Chicago-area physician group. The devices contained patient information used for administrative purposes.

INFORMATION COMPROMISED

Names, addresses, dates of birth, Social Security numbers, diagnoses, medical record numbers, medical service codes, health insurance information

BUSINESS ASSOCIATE INVOLVED

None



Health Net®

1.9



MILLION

PEOPLE AFFECTED

DATE: JANUARY 2011

HERE’S WHAT HAPPENED

Nine server drives for the managed care organization went missing from a data center managed by IBM. Personal information of some former and current Health Net members, employees and healthcare providers was on the drives.

INFORMATION COMPROMISED

Names, addresses, health information, Social Security numbers, financial information

BUSINESS ASSOCIATE INVOLVED

IBM



1.7



MILLION

PEOPLE AFFECTED

DATE: DECEMBER 2010

HERE’S WHAT HAPPENED

Computer backup tapes from the New York provider were stolen from a truck GRM was using to transport them to a secure storage location.

INFORMATION COMPROMISED

Names, addresses, Social Security numbers, patient medical histories, occupational/employee health information

BUSINESS ASSOCIATE INVOLVED

GRM Information Management Services

All statistics are from HHS Office for Civil Rights breach tally, except for the Community Health Systems incident, which is not yet on the list.

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

View this infographic online

<http://www.databreachtoday.com/top-5-health-data-breaches-a-7227>

ISMG Network Resources

<http://www.healthcareinfosecurity.com/healthcare-fresh-target-for-hackers-a-7207>

<http://www.healthcareinfosecurity.com/interviews/stopping-laptop-breaches-key-steps-i-2179>

<http://www.healthcareinfosecurity.com/blogs/breach-prevention-using-nist-framework-p-1723>

<http://www.healthcareinfosecurity.com/surveys/state-healthcare-information-security-today-s-23>

Data Breach

Prevention. Response. Notification. TODAY