Healthcare Data

Breaches & *Vulnerabilities*

and what you can do about them

2014

Contents

JDL HealthTech
HIPAA-Compliant IT Services

Overview

In 2014, across all industries, 292 data Breaches were reported to the Privacy Rights Clearinghouse, affecting 67.6 million Records.

(An increase from 256 Breaches exposing 953,220 Records in 2013.)

In 2014, across all industries, half of all Breaches were electronic (50%). However, **99%** of the affected Records were electronic.

In **Healthcare**, 93% of all affected Records were electronic. It is vital to effectively **secure and protect** your ePHI at all times!

93% of healthcare records breached in 2014 were electronic.

This report is compiled annually by JDL HealthTech as a convenience for our healthcare provider community

In 2014, more data breaches were reported in the Business sector than in the Healthcare industry.

In **Business**, 114 Breaches affected 59.5 million Records.

39%

The **Business** sector led both statistics in 2014, with **39%** of all Breaches affecting **88%** of all Records.

In **Healthcare**, 75 data Breaches affected 4.9 million Records.

26%

Healthcare was responsible for **26%** of all Breaches in 2014, affecting **7%** of all Records jeopardized by all Breaches.

*Financial Services took Third Place in 2014 with **14%** of all reported data breaches.*

Reports by Industry

Incidents reported to Privacy Rights Clearinghouse in 2014

Industry or Sector	Number Breach Reports	Number Records Affected	Percent of Total Breaches
Business	114	59,511,581	39%
Healthcare	75	4,895,066	26%
Financial	42	344,924	14%
Education	28	1,063,890	10%
Government	27	1,725,755	9%
Non-Profit	6	55,030	2%
All Reports	292	67,596,246	100%

HEALTHCARE DATA BREACH REPORTS SINCE 2010

Healthcare's annual share of data breaches has shifted recently from one-third of total breaches reported to one-quarter in 2014

2010 31% 2011 34% 2012 33% 2013 44% 2014 26%

Top Vulnerabilities

Unintended **disclosure** of PHI or other private data

23%

Of all breaches in Healthcare in 2014

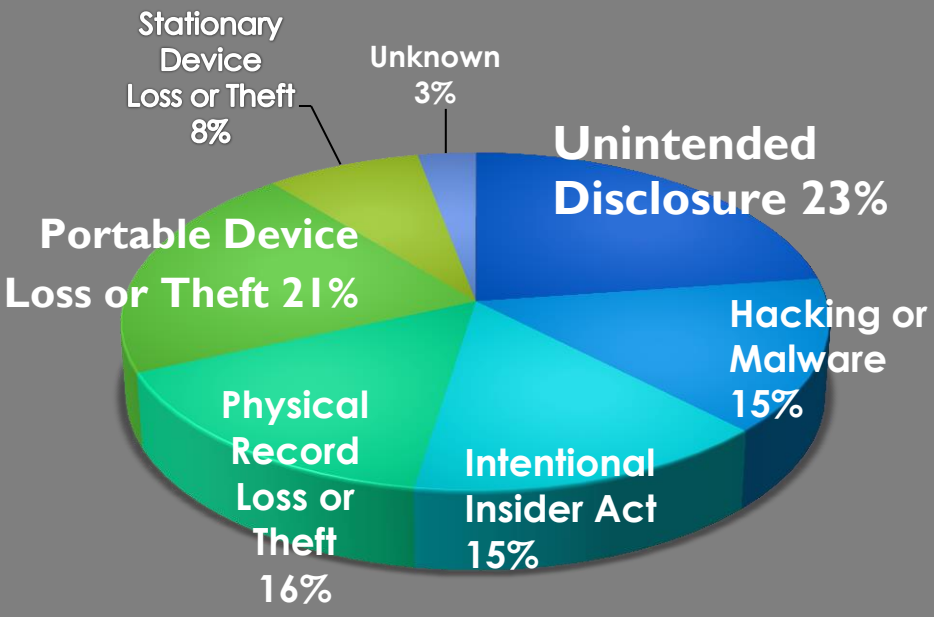
Loss or theft of **portable** computing devices

21%

Of all breaches in Healthcare in 2014

Source: Privacy Rights Clearinghouse

Causes of All Healthcare Data Breaches in 2014



ePHI and Portable Devices must be made Secure!

- For HIPAA compliance
- For patient protection
- To avoid fines and negative publicity
- For peace of mind

Source: Privacy Rights Clearinghouse

How Unintended Disclosures Occur

- **Patient information is accessible by staff who do not 'need to know' for their job/title**
- **Computer screens face common or public areas, and/or do not use screensavers**
- **Staff conversations can be overheard by patients or staff who do not 'need to know'**
- **Patient bills or information are mailed to the wrong patients**
- **Prescriptions faxed or emailed to incorrect address (not pharmacy)**
- **Employees visit unsecured websites that install malware on computer(s) to siphon off patient data for sale**
- **Employees click on links in emails that allow hacker entry or installation of malware**
- **All staff use same password for access**

Are You Guilty?

How Portable Devices Are Lost or Stolen

- Thumb drive containing ePHI gets lost
- Smartphone used for both professional and personal business is misplaced
- Laptop is stolen from vehicle
- Tablet goes missing from office

- Devices are not password-protected
- Devices are not encrypted
- Security protections are out of date
- Security protections have not been turned on
- Security protections are residential-grade, not commercial or enterprise-grade
- Data cannot be wiped from the device remotely in case it is lost or stolen
- Device user regularly auto-connects to public Wi-Fi hot spot, such as coffee shop

Are You Guilty?

HUMAN NEGLIGENCE

Caused 83% of Data Breaches in Healthcare in 2014

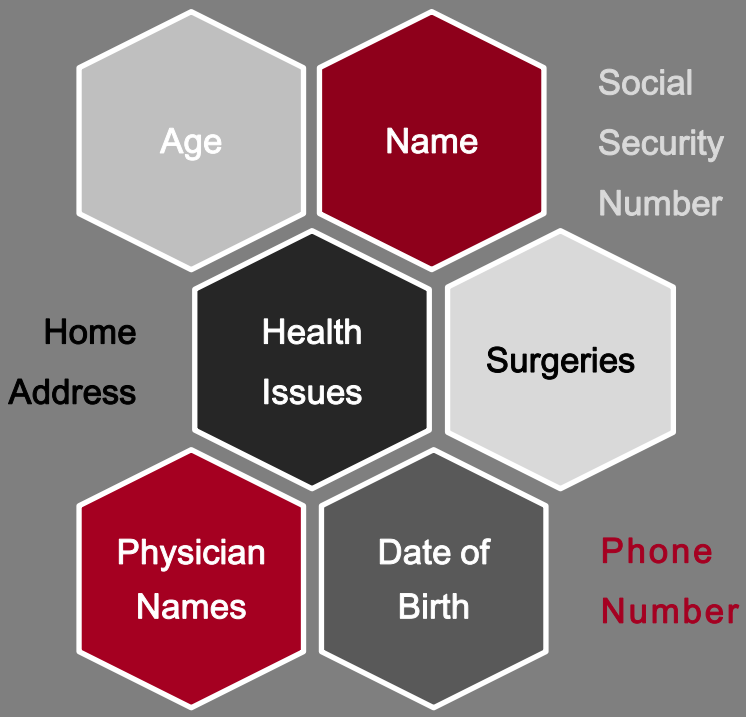
Cause of Breach	Breaches
Unintended Disclosure	17
Portable Device Loss or Theft	16
Physical Record Loss or Theft	12
Intentional Insider Action	11
Hacking or Malware	11 *
Stationary Device Loss or Theft	6
Unknown Cause	2 *
TOTAL BREACHES IN 2014	75

* Only these 13 breaches due to Hacking, Malware, or Unknown Causes are not directly attributable to Human Negligence. (Although the fact is many Malware infections are enabled by employees who click on links or websites they are not familiar with.)

The other **62 data breaches in 2014,** or **83%,** can be directly attributable to Human Negligence in one form or another.

The single greatest cause of Human Negligence is lack of adequate employee training in security and privacy precautions.

Patients Pay a High Price For Our Negligence



Protected health information (PHI) that is exposed or breached can be used to obtain credit cards and open bank accounts using victims' personal data.

Stolen data can lead to identity theft, missed job opportunities, increased medical insurance rates, and legal problems for victims.

HIPAA PENALTIES

Civil monetary penalties

Tier	Penalty
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

Criminal penalties

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

Penalties are established by HITECH Act and imposed by Dept. of Health & Human Services Office for Civil Rights (DHHS OCR).

Table from University of Indiana Advanced Biomedical IT Core website.

2014 Penalties *for* Violations

Throughout 2014, even the smallest HIPAA violations suffered serious consequences, as sampled below. This will continue.

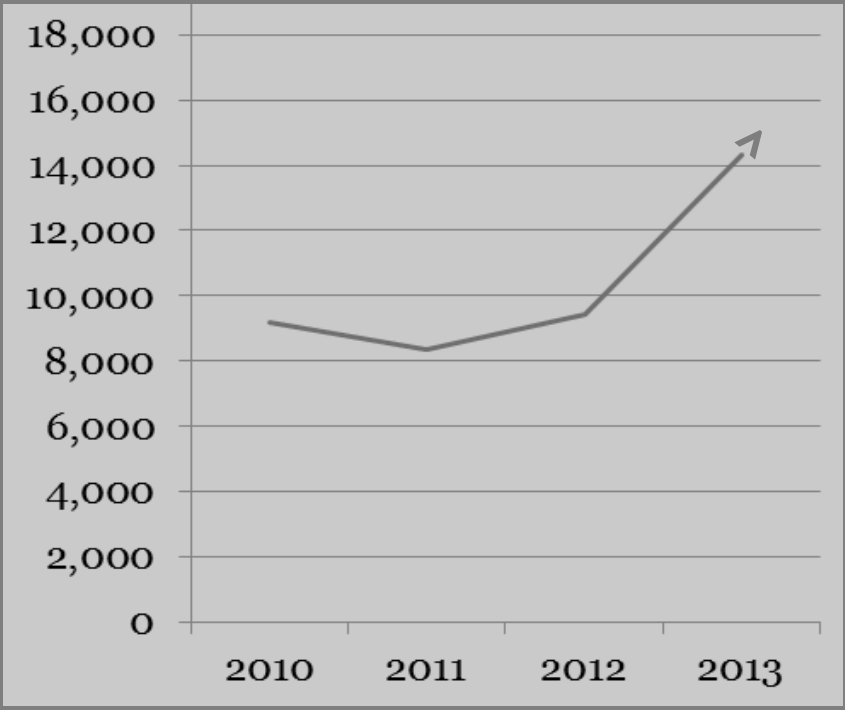
$250,000. Amount QCA Health Plan Inc. of Arkansas paid to OCR after laptop was stolen from employee car. Laptop contained 148 patients' data. QCA was cited for multiple HIPAA violations, and must complete corrective action plan imposed by OCR, including Security Risk Assessment.

$150,000. Amount paid to OCR by Anchorage Community Mental Health Services for ignoring its own documented security policies, including risk identification and regular software updates. Malware entered their system and breached 2,743 patients' unsecured ePHI. Must also complete corrective action plan imposed by OCR.

$12,000. Amount Comfort Dental of Kokomo, Indiana paid to State of Indiana for violating state privacy and HIPAA laws by disposing of 60 boxes of patient records in Indianapolis dumpster. Action by OCR pending. Dentist/owner has retired.

Source: DHHS OCR Website

HIPAA Violations Reported to DHHS Are UP!



Self-reporting of Violations became mandatory in 2009.

Source: DHHS Office for Civil Rights.
Data for 2014 not yet available.

2014 *Summary*

Healthcare no longer leads all industries in number of **Breaches**, but still accounts for one-quarter of all breaches (26%).

Healthcare also owns second place in the number of **Records** exposed (7%).

Most Healthcare breaches (23%) are caused by **Unintentional Disclosure** of PHI or other private data.

Theft or loss of **Portable Devices** like tablets, smartphones and laptops accounts for 21% of Healthcare breaches.

83% of all Healthcare breaches are caused by **Human Negligence**, which primarily stems from inadequate training.

A violation affecting just **148 records** has incurred an OCR penalty of $250,000.

Additional FACTS

The DHHS Office for Civil Rights is funded and authorized to conduct compliance audits **at random.**

It only takes **ONE complaint** from a patient or former employee to have your practice audited. (Are you prepared for that?)

Healthcare providers should ONLY use **Business Associates** who have proven their HIPAA compliance.

All providers MUST designate a HIPAA **Compliance Officer** and enable all necessary training.

All employees MUST receive **HIPAA Training** and, refresher training, and more training.

Every compliance action you take MUST be **documented** for future audit.

Don't Gamble
With Compliance

Now, you can protect your PHI, achieve HIPAA compliance, pass your OCR audit, avoid penalties, and gain peace of mind …

with these and other award-winning services from JDL HealthTech, the #1 provider of HIPAA-compliant IT services in Florida:

Security Risk Assessments
HIPAA Compliance Training
Encryption
ePHI Access Monitoring
Managed IT Services

JDL HealthTech
HIPAA-Compliant IT Services

JDLHealthTech.com **888.493.7833**