DataMatrix Medical

The Impact of Physician Error on Patient Data Security

2

The Impact of Physician Error on Patient Data Security

Understanding The Effect of Employee Error on Healthcare Data Incidents and Breaches

In recent years, protecting private patient information has become more difficult than ever. As technology continues to advance, the amount of healthcare security incidents and data breaches has significantly increased.

> ***In fact, the healthcare industry is roughly 7x more likely to elicit a causal error in cybersecurity incidents than any other industry.***

And what is the cause of said errors? Healthcare employees. According to the 2018 Verizon Data Breach Report, 58% of all incidents involved insiders—meaning people who work within the healthcare industry.

In this guide, we will:

- *Discuss key terms involved with incidents and breaches, as well as detailing the difference between an incident and breach.*
- *Display key statistics in the form of an infographic.*
- *Explain how these statistics may impact your practice.*

3

Incidents and Breaches: What You Need to Know

Before diving into our infographic below, we thought it was necessary to cover many of the terms you'll come across. At your practice, you and your team are likely familiar with these terms. However, we want to discuss what they mean in terms of data incidents and breaches.

Security Incident vs. Data Breach

An incident is an anomalous occurrence that discloses unauthorized personal data, without the loss of data—resulting in no serious impact on the practice.

A breach is also an anomalous event that discloses unauthorized personal data. However, a breach results in lost data and damage to the practice.

An incident does not always require a report to HIPAA. A breach, on the other hand, is in direct violation of HIPAA regulations and will warrant more serious implications.

Categorizing Incidents and Breaches

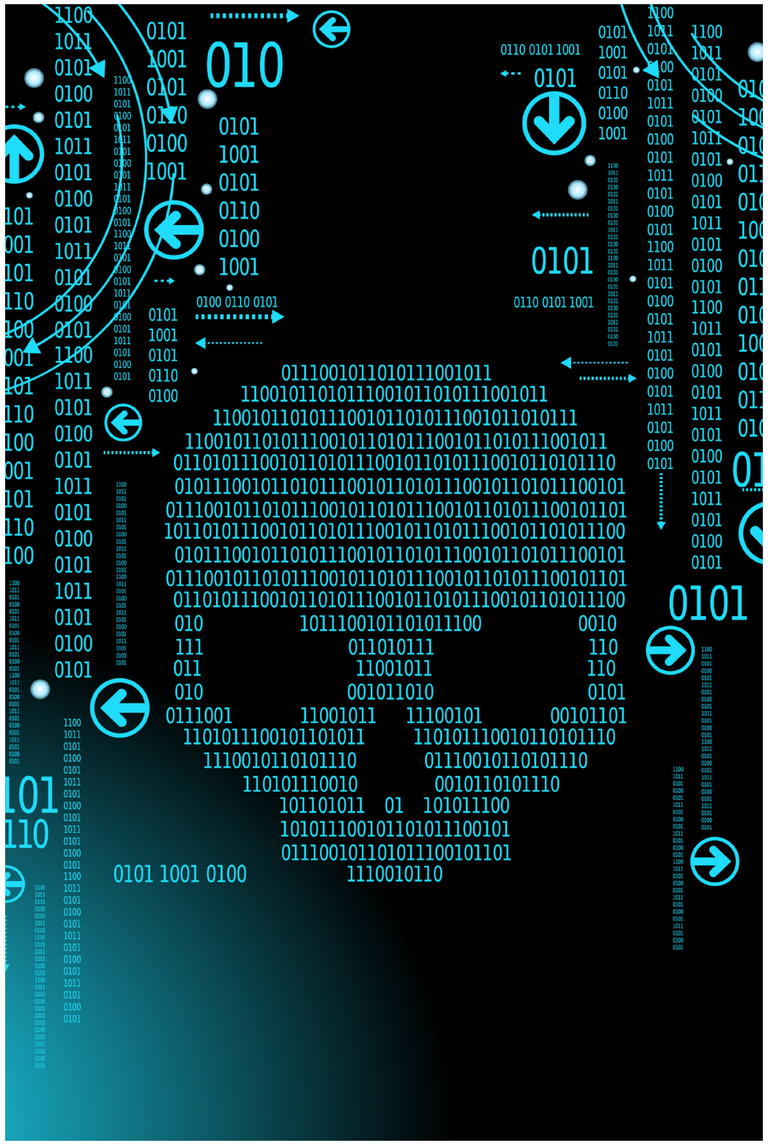
When protected health information (PHI) is violated, it is normally categorized into three levels of intent:

- *Intentional, malicious*
- *Intentional, not malicious*
- *Unintentional*

Intentional, malicious means that the incident occurred as a result of malicious actions that were intended to cause harm.

Intentional, not malicious occurs when the user intends to violate PHI, but does not intend to cause harm. An example would be an employee snooping for unauthorized information about a loved one, friend, celebrity, etc.

Unintentional is the most common form of incidents and breaches. When an incident is unintentional, the employee may unknowingly violate PHI by sending patient information to the incorrect recipient, misdirecting faxes, etc.



What Actions Constitute A Threat?

Actions that violate PHI and constitute a security incident or data breach are as follows:

Error

An incident that is caused by unintentional actions, resulting in a compromised attribute of a security asset.

Primary causes: Misdelivery, disposal error, loss, publishing error and misconfiguration

Misuse

Incidents such as privilege abuse and data mishandling that involve unapproved or malicious use of organizational resources.

Primary causes: Privilege abuse, data mishandling and possession abuse

Physical

A physical incident occurs when data goes missing either through misplacement or malice.

Primary causes: Theft, snooping and tampering

Hacking

An incident caused by a threat actor who gains unauthorized access to a user's device or system.

Primary causes: Stolen credentials, brute force and use of a backdoor or C2

Malware

An incident caused by malicious software, such as opening an attachment or link in a spam email, that enables a threat actor to private systems and data.

Primary causes: Ransomware

Social

A social incident is the result of a threat actor targeting a healthcare individual to gain access to their private data.

Primary causes: Phishing

These six types of threats are the primary causes of incidents and breaches all over the world. Error and misuse are the most common, however they all pose serious threats to the security of patient data.

Below, you will find the statistics behind these threats, with further explanation of how these actions can detrimentally impact your own practice.

Is It Worth The Risk?

How Healthcare Employees Threaten Data Security

"Healthcare is the only industry where internal employees pose the biggest threat to an organization."

58% OF ALL INCIDENTS INVOLVED EMPLOYEE INSIDERS

48%
WERE INFLUENCED BY FINANCIAL MOTIVATORS

31%
VIOLATED PHI FOR FUN OR CURIOSITY

10%
OF EMPLOYEES COMPROMISED PATIENT DATA FOR CONVENIENCE

Most breaches were caused by paper documents and databases.

49%
OF ALL HACKING INCIDENTS WERE DUE TO STOLEN CREDENTIALS.

63%
OF ALL SECURITY INCIDENTS AND DATA BREACHES WERE CAUSED BY

ERROR & MISUSE

(misdelivery, disposal error, loss)
(privilege abuse, data mishandeling, possession abuse)

Ransomware infections accounted for 70% of malware incidents.

7

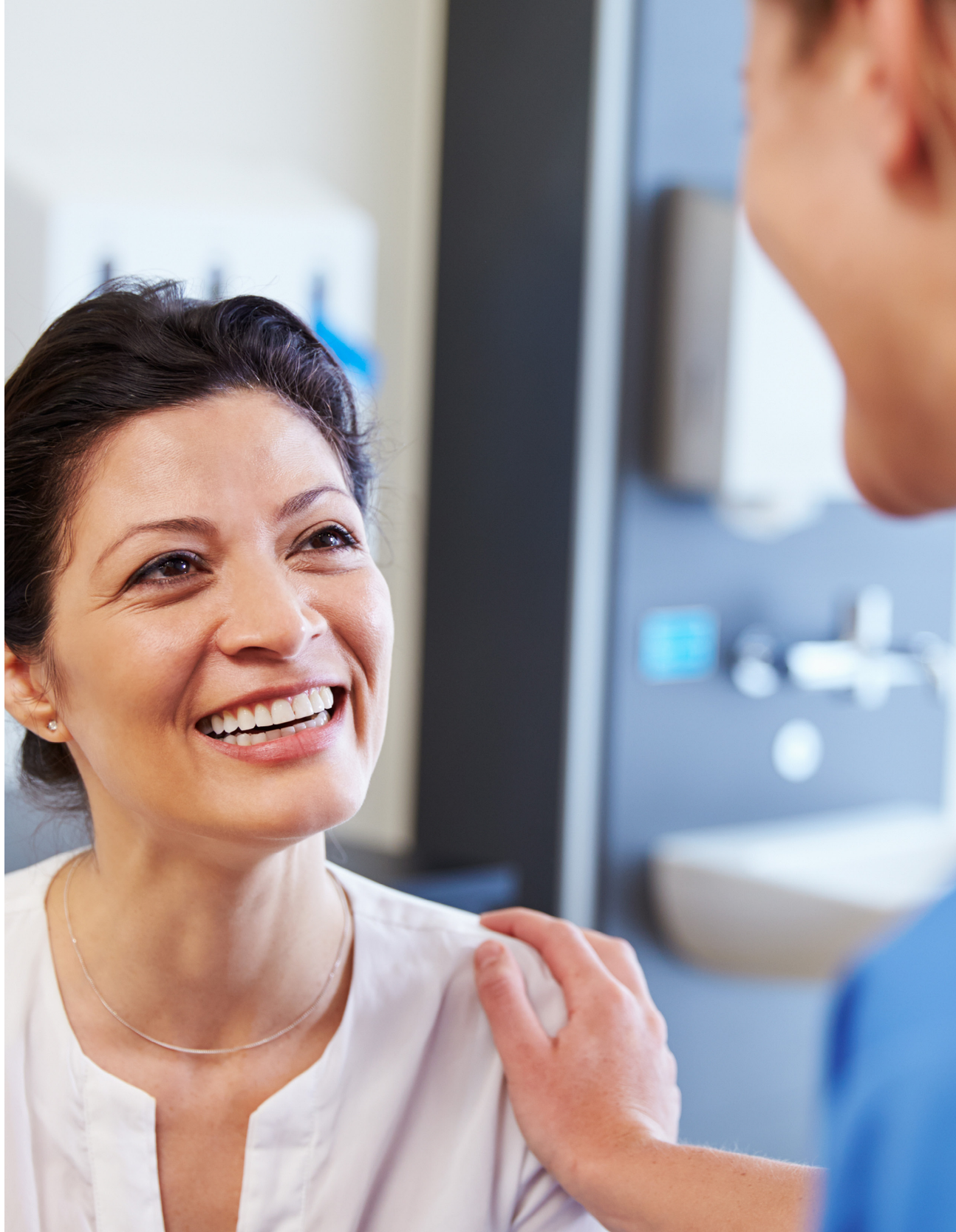
What These Statistics Mean For Your Practice

Looking at the numbers, you can see how easily protected patient information can be compromised. Oftentimes, private patient data is accessed due to unintentional negligence—but these simple mistakes can be so easily prevented.

Don't let your practice suffer due to a lack of secure patient data.

Moving forward, remember these key takeaways:

- *Over half of healthcare incidents and breaches were caused by employees.*
- *Employee error and misuse were the top two causes of security incidents and data breaches.*
- *Surprisingly enough, paper documents are one of the leading causes of incidents and breaches.*
- *Ransomware infections caused 70% of malware incidents.*



Continue to educate your staff on the importance of patient data security. While these statistics are startling, they can be reduced with effort, training, attention and time.

At DataMatrix Medical, we know the value of protecting patient data. That's why we have developed each and every one of our services around securing patient information. When you trust us with your transcriptions, billing, coding and more, we promise to put patient data protection at the forefront.

All of our solutions are **HIPAA compliant** and **secure**, so you'll never have to worry about patient data being at risk.

To learn more about how our solutions can help prevent patient data from being compromised, start a free, no-obligation two-week trial and put our services to the test.

Request Your Two-Week Free Trial

DataMatrix Medical

https://www.datamatrixmedical.com

866-219-2620

info@datamatrixmedical.com

Sources:

https://enterprise.verizon.com/resources/reports/dbir/

https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/

https://www.norcal-group.com/library/71-of-cybersecurity-incidents-in-healthcare-involve-employee-actions

https://www.radarfirst.com/blog/looking-good-on-paper-benchmarking-data-reveals-importance-of-paper-incidents-across-industries

https://www.asi.com.au/blog/difference-data-breach-security-incident/

https://www.calyptix.com/hipaa/top-5-causes-of-data-breaches-in-healthcare/