Fusion
MEDICAL STAFFING

UNDERSTANDING *Data Security*

Six ways breaches happen and how you can prevent them.

Healthcare has a problem

DATA BREACHES IN HOSPITALS ARE EXPENSIVE AND BECOMING MORE COMMON.

There has been almost
ONE BREACH
per day since 2015.[1]

Data breaches cost approximately
$380 PER STOLEN RECORD
in 2017.[2]

Since 2015,
MORE THAN 41%
of the U.S. population has had some of their health information exposed.

Since 2015,
135,060,443
healthcare records have been exposed or stolen.

The good news is some of these breaches stem from human negligence or lack of training. How in the world is that good news? It means you have more control than you may realize.

IN THIS EBOOK, WE'LL TALK ABOUT HOW BREACHES CAN HAPPEN AND HOW YOU AND YOUR STAFF CAN HELP PREVENT THEM.

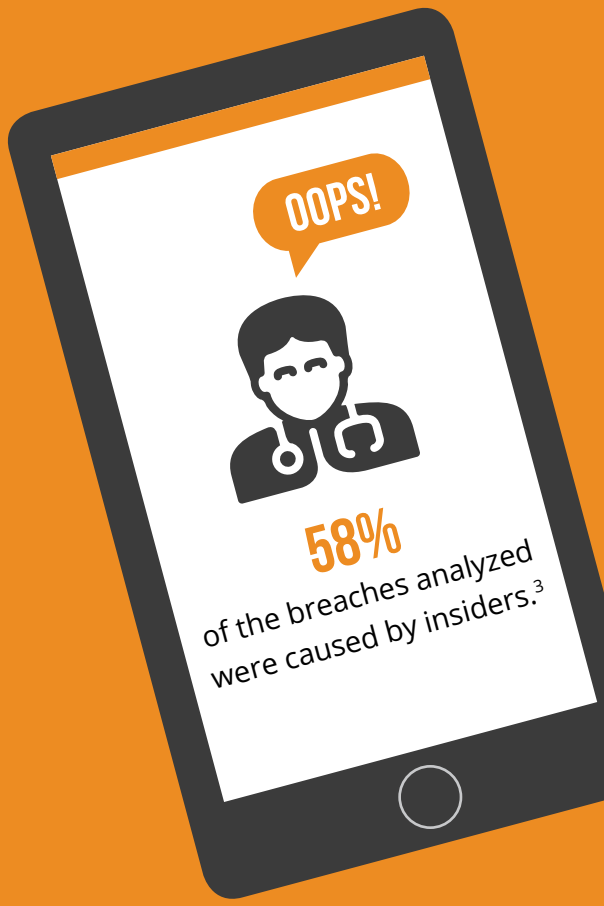
How breaches happen

THE CALL IS COMING FROM INSIDE THE HOUSE!

In 2018, Verizon analyzed 1,368 healthcare data breaches and incidents where protected health information (PHI) was exposed but not necessarily compromised.

While unfortunate, this stat makes sense. The people handling sensitive healthcare data on a daily basis are medical professionals, not IT experts. Their days, like yours, are high-stress and fast-paced. Sometimes they bypass security measures as a way to save time, but as many healthcare companies have learned the hard way, it ends up costing more in the end.

Keep reading to learn six ways healthcare staff are putting their data at risk, sometimes without even knowing it.



NUMBER ONE

Internet misuse

FIREWALLS ARE OUR FRIENDS.

Internet usage at healthcare organizations is locked down pretty tight—or so you thought. Many staff still find ways to go around security measures by using private or anonymous browsers to do things that obviously aren't allowed, like:

- Online gambling
- Viewing adult content
- Playing games

Some staff go around security measures to make their jobs easier. The intention is good, but the outcome could be very bad. They might use online programs that require email sign-up or download apps to help them:

- Share files
- Keep computer screens from sleeping
- Make it easier to take screenshots

PREVENTING INTERNET MISUSE:

Inquire.
Ask your staff if they require additional tech to simplify their jobs. If file sharing is a common issue, maybe a secure option could be rolled out to all.

Review.
Regularly go over your internet use policy with staff. If you don't have one, work with your security decision-makers to develop one.

Monitor.
Work with IT to decide how best to track misuse, whether it's monitoring online traffic, browsing your system's cache, etc.

NUMBER TWO

Errors

THINGS THAT MAKE YOU SAY, "OOPS."

Usually unintentional, always problematic, both human and technical errors can lead to vulnerabilities in the network. Technical errors typically require a technical solution, but human error can be lessened with awareness.

Human errors include:

- Sending an email or physical mail containing PHI to the wrong recipient
- Filing paperwork or entering data incorrectly (physically or digitally)

Preventing human errors:

1. **Say "why."** Explain the risks associated with a seemingly small mistake.
2. **Facilitate.** Give employees a low-shame way to report these small errors, so reporting becomes part of workplace culture.
3. **Back it up.** It's a best practice in IT to have data backed up in at least one place.

TERM TO KNOW:

PHI: Protected health information or personal health information. This includes patient demographics, medical history, lab and test results, mental health information, insurance information, and more. PHI is protected by HIPAA.

NUMBER THREE

Malicious behavior

MORE MONEY, MORE PROBLEMS.

A recent study revealed that nearly one in five, that's 18%, of healthcare employees surveyed would be willing to sell confidential data. The act of selling or stealing data could involve giving out login credentials, installing tracking software, or downloading information to a portable device. Insiders might also use this information for personal gain in the way of identity theft and fraud or stealing information to take to a new employer.

Preventing malicious behavior:

- **Training.** Ensure that all employees are aware of what behavior constitutes a cybercrime.
- **Tracking.** Studies have shown that training alone isn't enough to deter this behavior. You must also work with IT to track suspicious online behavior.

IT'S HAPPENING:

24% of survey respondents knew someone who sold their login credentials to an outside source or stole data themselves.[4]

HIRE THE BEST:

At Fusion, we perform extensive background checks to ensure everyone we work with is responsible and trustworthy.

NUMBER FOUR

Privilege abuse

NO UNAUTHORIZED EMPLOYEES ALLOWED.

When people access data or health records without proper authorization, it's called privilege abuse. It's when you use someone else's login credentials or handle physical records you're unauthorized to see.

Security precautions like these may seem like a barrier to caring for patients because they take more time and involve more people rather than just doing something yourself. But information security is a crucial reason for specific authorizations.

Preventing privilege abuse:

- **Reinforce.** Remind staff why authorization protocol is necessary.
- **Protect.** Remind staff that all login credentials are private, and passwords should never be written down for others to find.
- **Inform.** Make sure all staff is aware of who to speak to should they need access to information they can't currently access.

EASY TARGET:

21% of surveyed healthcare employees said they keep their login credentials written down near their computers.[5]

NUMBER FIVE

Phishing

STRANGER DANGER BUT FOR YOUR INBOX.

Phishing continues to be a threat to healthcare information security, particularly phishing emails. And while anti-spam filters help, bad emails still manage to get through. That's because the onus is on individuals checking their inboxes to know what's okay to click on. Not only could phishing lead to an insider providing important login credentials, but it could introduce ransomware or other malware into the network.

Elements of a phishing email:

- Urgent or threatening language
- Lots of exclamation marks in the subject line
- Request for personal information or login credentials
- Links to a site you're not familiar with
- Generic greeting message
- Noticeable spelling and grammar errors or random capitalization
- Includes an attachment

Preventing phishing:

It's important to teach staff how to spot phishing and what to do when they receive an email like this. It could be as simple as forwarding the email to IT.

TERMS TO KNOW:

Ransomware.
A type of malicious software (malware) that takes control of stored data on your computer or other device and demands payment (ransom) in order to get it back.

Phishing emails.
Fraudulent communications from companies that seem reputable but are trying to lure you into revealing personal information like passwords and credit card numbers.

NUMBER SIX

Theft

VICTIMS OF OUR OWN DEVICES.

Laptops. Tablets. Smartphones. These portable computers are vital to the work you do every day—and they're pretty valuable in their own right. Add access to PHI, and you've got one extra-enticing target. There are two ways you can protect stolen devices from becoming portals to even more costly theft.

Preventing theft:

- **Encryption.** This is a must-have in the BYOD (bring your own device) world we live in. Encryption is a way of encoding and protecting information so only certain individuals can access it and it's harder to hack.
- **A mobile device policy.** Create an internal policy that outlines appropriate mobile device use. It should include things like password-protecting your phone and only using secure Wi-Fi networks on the go. Regularly train employees on the do's and don'ts.

BIG PROBLEM:

Over 33% of all large breaches since 2009 have involved unencrypted devices. These incidents put over 50% of all health records at risk.[6]

Mandatory regulation

THE HIPAA SECURITY RULE.

The Department of Health and Human Services (HHS) wrote the HIPAA Security Rule in 2003 to establish national standards for protecting PHI by providers, payers, and other entities. A long list of technical, administrative, and physical safeguards are required by the Security Rule. The safeguards were designed with scalability in mind so both small companies and massive corporations could abide by the rule.

You can learn more about the Security Rule and download a free risk assessment tool to help identify vulnerabilities and potential HIPAA violations at **healthIT.gov**.

Raise the red flag

THE SIX WAYS INSIDERS ARE PUTTING DATA AT RISK.

In this eBook, we've covered a lot of considerations for protecting PHI, primarily those that involve the day-to-day activities of your staff. Research has shown that the most effective methods for combatting data theft are a combination of employee education and technical precautions. As you look at the issue from every angle, here's a recap of the six things you can talk about with your team.

1. Internet misuse
2. Human and technical errors
3. Malicious behavior
4. Privilege abuse
5. Phishing
6. Device theft

Fusion

MEDICAL STAFFING

Your partners in protection

Our job at Fusion is to make your job easier, which is why we made this eBook. Ultimately, the healthcare profession is all about caring for the communities you serve. Data security is an important way to continue patient care behind the scenes.

LET US KNOW HOW WE CAN HELP YOU

877-230-3885 | info@fusionmedstaff.com

[1] https://www.hipaajournal.com/security-breaches-in-healthcare-in-the-last-three-years/

[2] https://healthitsecurity.com/news/how-much-do-healthcare-data-breaches-cost-organizations

[3] https://www.hipaajournal.com/verizon-phi-breach-report-healthcare-insider-breaches/

[4] https://newsroom.accenture.com/news/one-in-five-health-employees-willing-to-sell-confidential-data-to-unauthorized-parties-accenture-survey-finds.htm

[5] https://www.accenture.com/us-en/blogs/blogs-losing-cybersecurity-culture-war

[6] http://www.healthcareitnews.com/news/5-ways-avoid-health-data-breaches