6 Tips for Medical Practice Cybersecurity

A guide to protecting your practice

71% of data breaches happen to businesses with less than 100 employees

"Data breaches don't just happen to large companies like Target and Home Depot, and patient data breaches don't only impact large healthcare organizations like Anthem Blue Cross and Banner Health."

Smaller medical practices are easy targets

Medical practices have the same valuable patient information, just less of it and with less protection. Practices spend less on cybersecurity than larger organizations. Cybercriminals often target medical practices because they have a lot of patient information that can be used for identity theft, tax fraud and other financial crimes.

Medical practices collect patient names, addresses, social security numbers, dates of birth, driver's licenses and insurance information. This information is everything a criminal needs to commit identity theft and other cybercrimes.

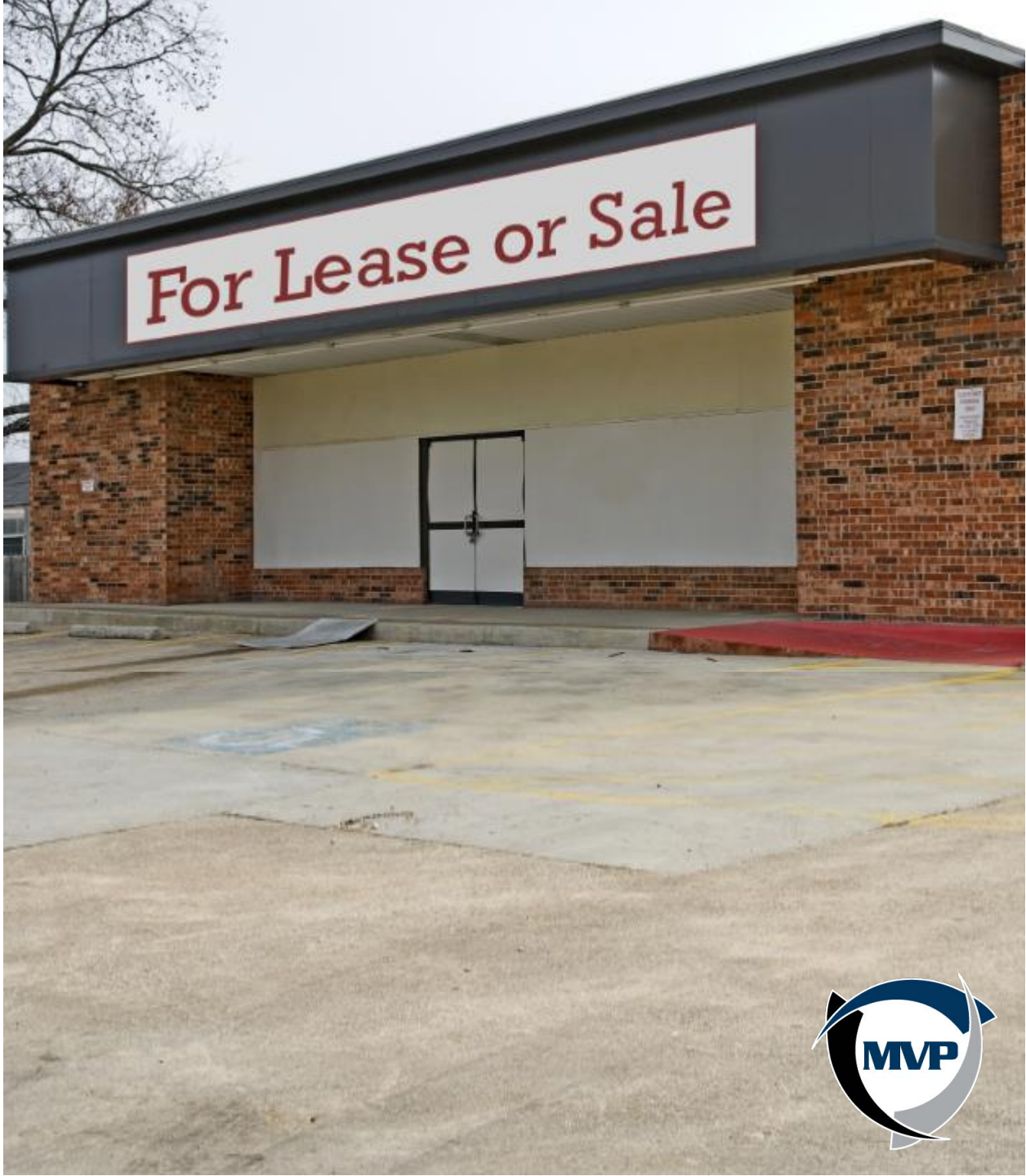
60% of small businesses go out of business after a data breach

Data breaches are expensive and can damage a practice's reputation.

Legal, IT, breach notification and identity monitoring expenses can add up quickly.

After a data breach, patients often leave a practice due to lack of trust, and negative publicity keeps newer patients from utilizing a practice's services.

Data breaches cause owners and employees emotional stress and anxiety.



Ransomware is a real threat to medical practices

Ransomware is a method of holding data hostage until a ransom or payment has been made to release the data. Ransomware is usually associated with fake emails called phishing emails that contain malicious attachments such as Microsoft Word documents or PDF files. Once these attachments are opened, a program locks or encrypts all the data on the workstation. Ransomware can spread to other workstations and servers on the network.

Criminals are targeting healthcare organizations from hospitals to medical practices. These criminals realize that it is easier to hold a medical practice's data hostage than it is to steal the data and use it. The risk of being caught spreading ransomware is much lower than traditional hacking or cybercrime.

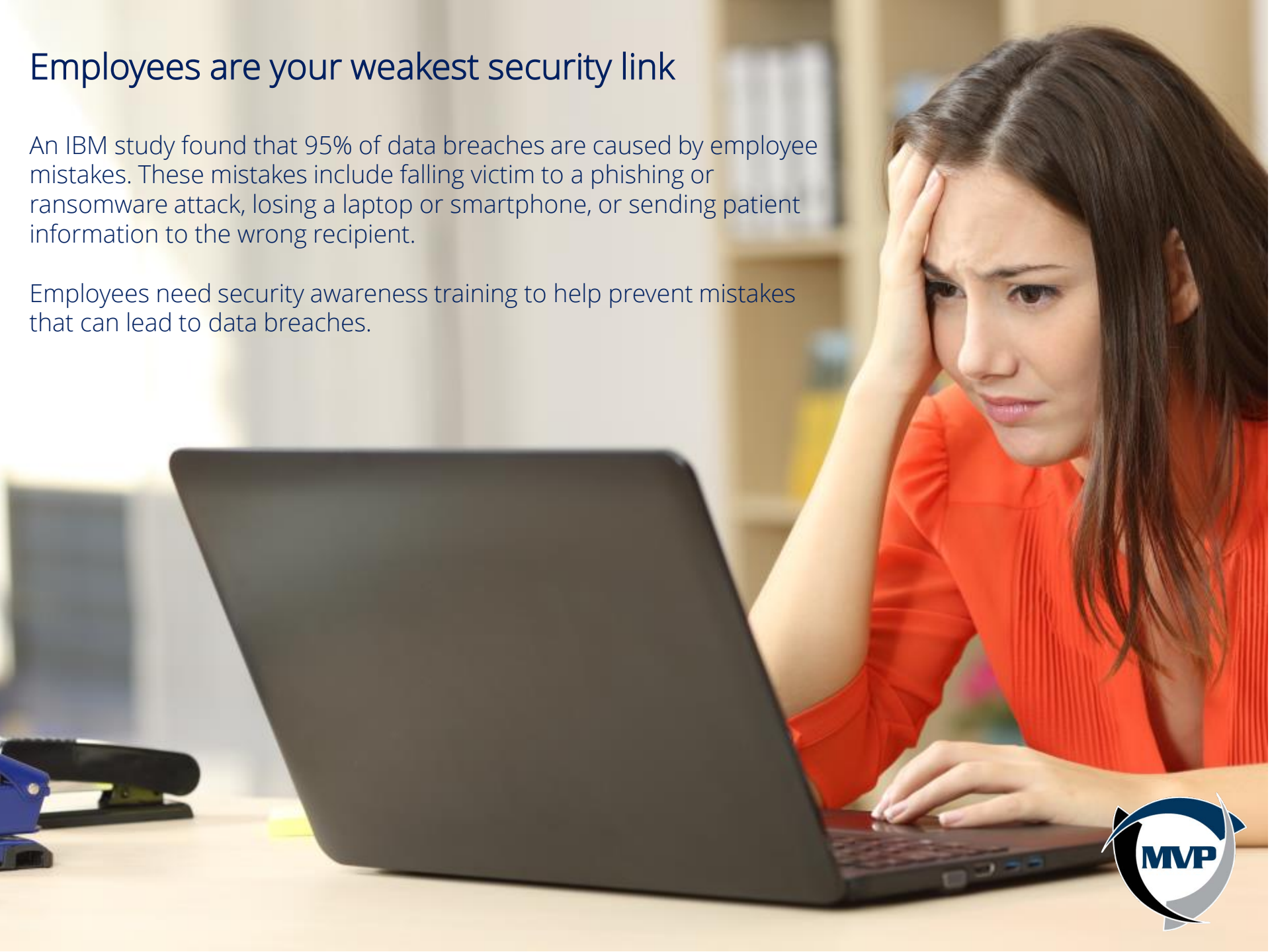
Hospitals and medical practices have been shut down for weeks as a result of successful ransomware attacks that have encrypted the entire network and made access to patient data impossible.

"It only takes one employee to fall for a phishing scam"

Employees are your weakest security link

An IBM study found that 95% of data breaches are caused by employee mistakes. These mistakes include falling victim to a phishing or ransomware attack, losing a laptop or smartphone, or sending patient information to the wrong recipient.

Employees need security awareness training to help prevent mistakes that can lead to data breaches.

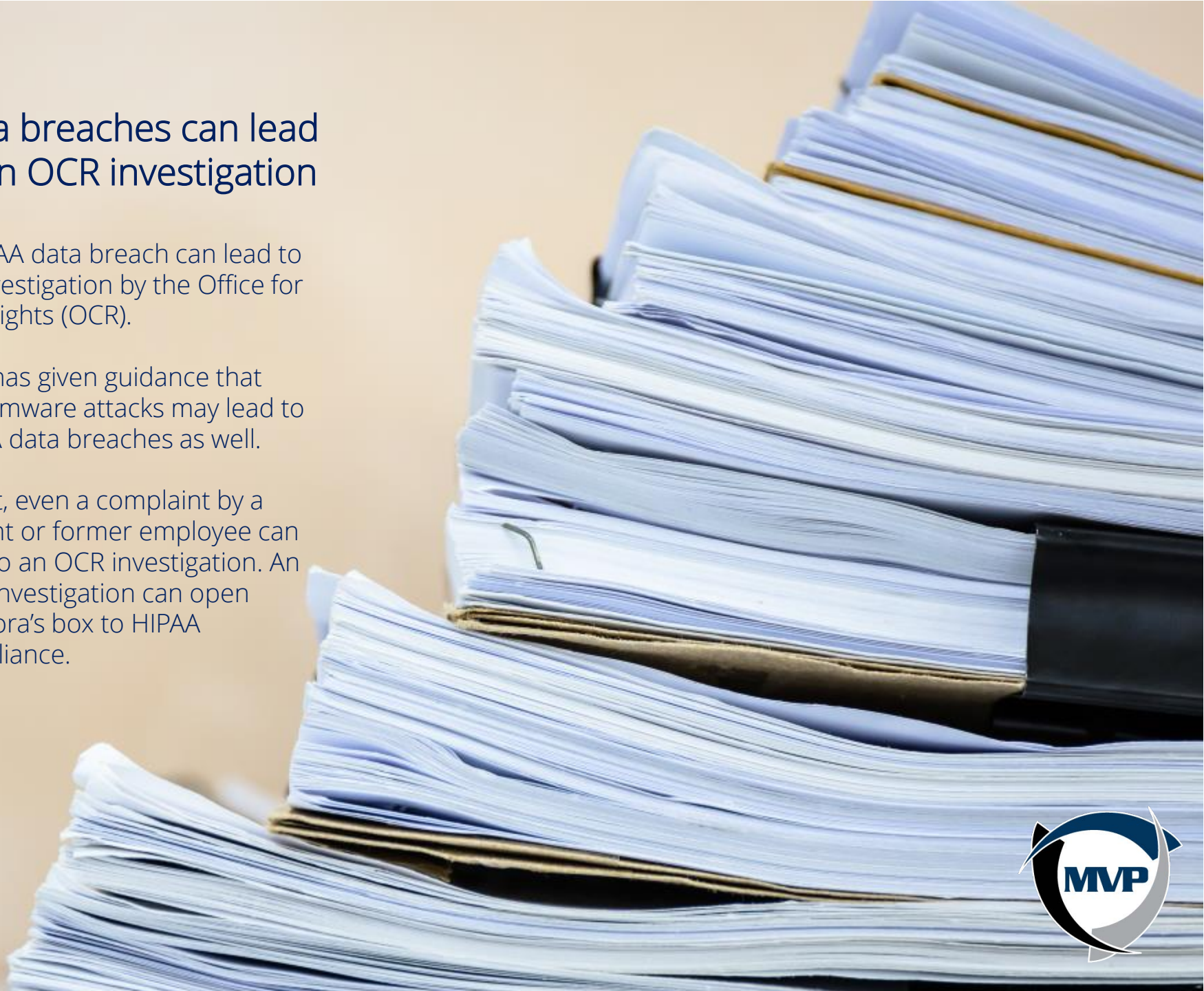


Data breaches can lead to an OCR investigation

A HIPAA data breach can lead to an investigation by the Office for Civil Rights (OCR).

OCR has given guidance that ransomware attacks may lead to HIPAA data breaches as well.

In fact, even a complaint by a patient or former employee can lead to an OCR investigation. An OCR investigation can open Pandora's box to HIPAA compliance.



Best Practices

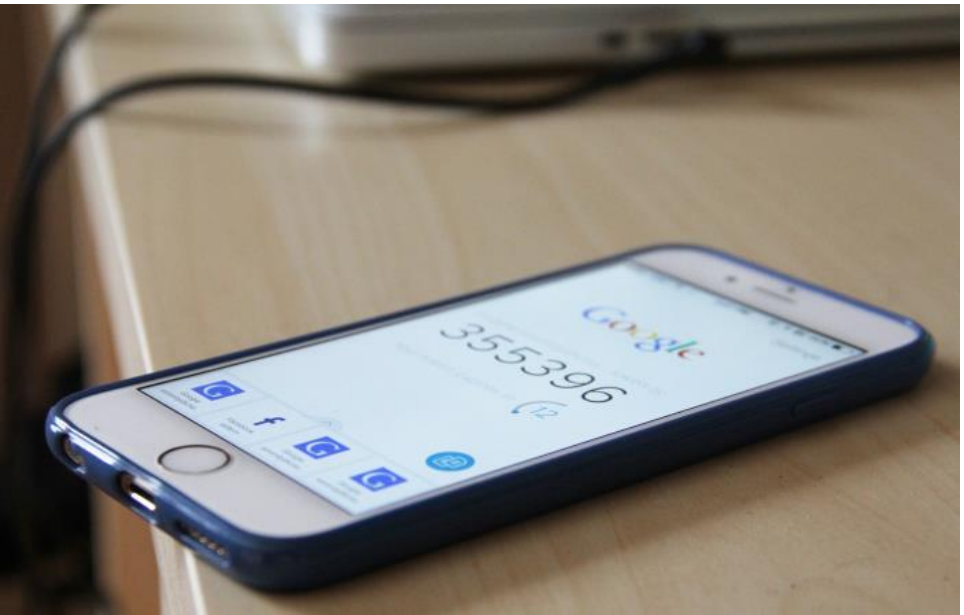
Although criminals are targeting the healthcare industry and smaller companies are frequent data breach victims, employing best practices can help protect your medical practice against cyberattacks and data breaches.

The following are best practices that you can take to minimize the chance of data breaches.

Secure passwords

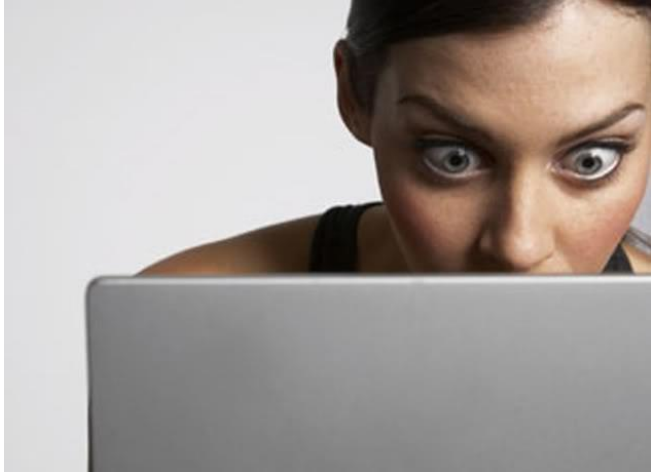
Passwords are the key to networks, patient information, online banking and social media.

Password best practices include:



- Use strong passwords.
  - ✓ **Make the password at least 8 characters long.** The longer the better. Longer passwords are harder for thieves to crack.
  - ✓ **Consider using passphrases**. When possible, use a phrase such as "I went to Lincoln Middle School in 2004" and use the initial of each word like this: "Iw2LMSi#2004".
  - ✓ **Include numbers, capital letters and symbols.**
  - ✓ **Don't use dictionary words.** If it's in the dictionary, there is a chance someone will guess it. There's even software that criminals use that can guess words used in dictionaries.
- **Change passwords.** Passwords should be changed every 60 to 90 days.
- **Don't post it in plain sight.** This might seem obvious, but studies have found that a lot of people post their password on their monitor with a sticky note.
- **Consider using a password manager.** Programs or Web services let you create a different very strong password for each of your accounts, but you only have to remember the one password to access the program or secure site that stores your passwords for you.
- **Consider using multi-factor authentication.** Set up multi-factor authentication that requires a code that is displayed on your phone. This way hackers cannot access an account without having physical access to your phone.

Insider threats



While cybercriminals and external threats should be cause for concern, insider threats are a leading cause of HIPAA data breaches.

Insider threats include employees or contractors that snoop or access patient information without authorization. Snooping on patient records may be malicious or simply done out of curiosity, but either way this unauthorized access is considered a HIPAA data breach.

Another insider threat includes employees or contractors that steal patient information. The stolen information is sold to a criminal third party who then uses it for identity theft or other crimes.

Employees and contractors are usually trusted individuals which makes preventing insider threats very difficult. To reduce the chance of insider threats, follow these steps:

- **Minimize the amount of access** that an employee or contractor has. These individuals should only have the minimum access needed to perform their job function.
- **Periodically review the level of access** for each of your employees and contractors.
- **Ensure that system auditing is in place**. System auditing records who accessed patient information, when it was accessed and what patient information was accessed.
- **Periodically review system audit logs** to look for red flags that might suggest unauthorized access by an employee or contractor. Without review of system audit logs, you are blind to what your employees may be doing.
- **Ensure that employees know that system auditing is in place** and that it is periodically reviewed. This might deter an employee or contractor from malicious activity.

Encrypt data

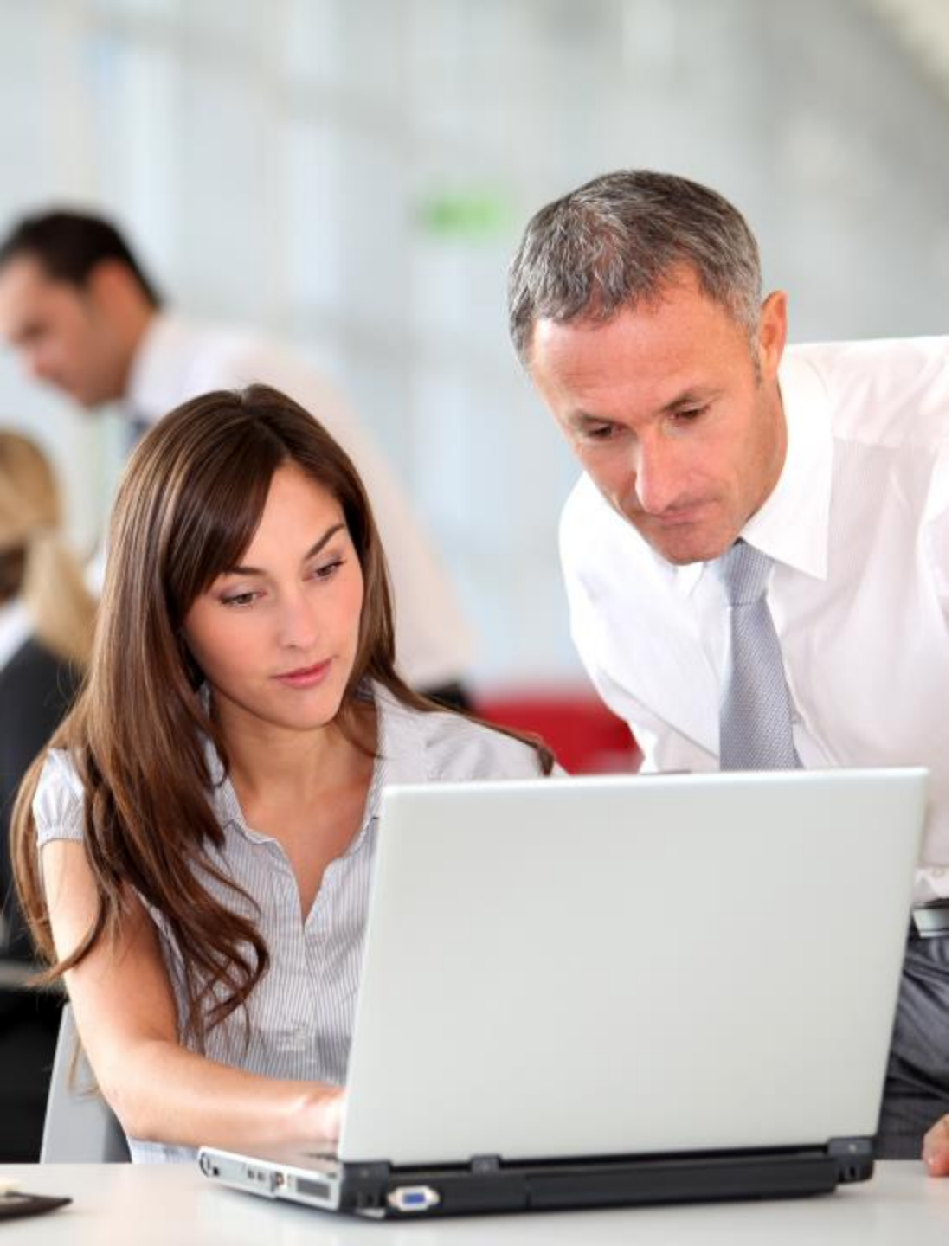
Lost laptops, smartphones and USB drives continue to cause HIPAA data breaches.

Many practices don't realize how much patient information is on mobile devices. Patient information could be in emails, spreadsheets, documents, PDF files and scanned images.

The best way to protect sensitive patient information is to use encryption. Encryption is a "safe harbor" under the HIPAA Security Rule. This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a reportable breach. Patients would not need to be notified.

Types of encryption

- **Mobile device encryption.** Laptops, smartphones and USB drives can all be encrypted. This will protect any data that is on these devices.
- **Email encryption.** Emails could contain patient information as well as other sensitive information and should be encrypted. Secure email will protect the data that is sent.
- **Secure texting**. Regular SMS texting does not protect data that is sent between phones. There are secure texting applications that encrypt data that is sent via text message. If your staff are texting patients or are texting other staff members about patients, you should look into secure texting applications.
- **Workstation encryption.** Like laptop encryption, desktops and workstations can be encrypted to protect any data stored on them. Workstation encryption is very important in the event of a break-in and theft of workstations. Without encryption, a stolen workstation may result in a HIPAA data breach.



Employee Security Training

95% of data breaches are caused by employee mistakes. It is critical to ensure that employees understand the risks to patient information and the threat of data breaches.

Phishing and ransomware are leading methods of attacks. Employees need to know how to spot phishing emails, phishing websites and the dangers of email attachments.

In addition to knowing how patient data can be disclosed and used, employees must be aware of how to protect electronic patient information. Training needs to go beyond bringing employees into a conference room and discussing HIPAA regulations. Training needs to take into account the dangers of hacking, stolen mobile devices, posting patient information on social media and other causes of data breaches.

OCR investigations usually require proof that all employees have been trained on an annual basis.

"95% of data breaches are caused by employee mistakes"

Data backup and disaster recovery

Backing up data will protect your medical practice from data loss due to damaged servers or malicious code such as ransomware.

A fire, flood, explosion or natural disaster can destroy systems that contain patient information. Having up-to-date data backups and a disaster recovery plan will help recover and restore patient information.

HIPAA regulations require that patient information be protected and available. Patient information cannot be lost or unrecoverable. Data backups ensure that data is recoverable.

It is recommended that automated backups occur that encrypt and copy data offsite.

Data backups should be periodically tested to ensure the data is able to be recovered.

"Only 6% of companies survive longer than 2 years after a significant data loss"

Perform a security risk assessment

A security risk assessment (SRA) is not only required under the HIPAA Security Rule, but is a critical step to understanding the risk to your practice and patient information.

An SRA will inventory patient information, identify how you are currently protecting the data and make recommendations on how to lower the risk to the data.

An SRA will help you to understand your risk of phishing scams and ransomware, the dangers of lost mobile devices, the risk of insider threats and how prepared you are in the event of a disaster.

Finally, it provides the documentation you need as evidence that you have considered all of the possible risks to patient information and have specific plans to lower them. You can't pass a HIPAA compliance audit or breach investigation without it.

From the Centers for Medicare & Medicaid Services (CMS):

"It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional."