Connecting practices to
EMERGING TRENDS.

CYBERSECURITY AND DATA BREACHES

Strategies to Mitigate Risk, Monitor Security, and Respond in the Event of a Cyberattack

THE DOCTORS COMPANY
medical ~~mal~~practice insurance

YOUR PRACTICE IS AT RISK

Every day, the threat of a data breach looms over your practice. An unencrypted laptop could be stolen. A vendor could inadvertently make your patient information publicly accessible. Or an employee could click on a seemingly harmless link—allowing hackers to hold your entire system hostage until you pay a ransom.

In today's healthcare environment, it's not a matter of if a breach will occur—it's a matter of when. Nearly 90 percent of surveyed healthcare organizations experienced a data breach over the past 2 years, and 45 percent experienced more than 5 breaches in that time.[1] Cyberattacks are now the leading cause of healthcare breaches, ahead of third-party mishandling of data, stolen or lost devices, and malicious insiders.[2] And cyberattacks are becoming more and more sophisticated as cybercriminals seek to exploit a lucrative market for personal health information (PHI).

This report will help you combat these dangers with specific recommendations to achieve the following:

- Comply with HIPAA Rules.
- Thwart Ransomware Attacks.
- Prevent Spear Phishing.
- Combat Password Theft.
- Scrutinize Your Vendors.
- Keep Cloud Data Safe.
- Respond Appropriately to a Breach.
- Prepare for Lawsuits.
- Plan Your Response Now.

By taking these steps you can enhance the security of your data, reduce your risk of a breach, and create a response strategy that will lessen the impact on your practice when a breach occurs.

COMPLY WITH HIPAA RULES

A data breach is the loss or unauthorized disclosure of personal information that can uniquely identify an individual associated with your practice. The individual can be a patient, employee, business partner, or vendor, and the information disclosed can create financial or reputational harm to the individual. A data breach can occur in any number of ways, including the theft of unencrypted electronic devices or physical records, the public distribution of personal records, or a cyberattack.

The repercussions of data breaches can be daunting. A business that suffers a breach of unencrypted PHI or a ransomware attack must report the breach to the U.S. Department of Health and Human Services Office for Civil Rights (OCR). This is the federal body with the power to enforce the Health Insurance Portability and Accountability Act (HIPAA) and issue fines.

A healthcare organization's brand and reputation are also at stake. The OCR routinely investigates providers who suffer breaches affecting more than 500 individuals, and it maintains a searchable database (informally known as the "Wall of Shame") that publicly lists all entities fined for breaches of this size.

⚠ Steps toward HIPAA compliance include:

- Identification of all areas of potential vulnerability, including:
  - Physical access to PHI, electronic health records (EHR), and paper records.
  - Desktop and network security.
  - Mobile devices.
  - Vendor access to your network—from your janitorial service to your cloud storage provider.
- Development and thorough documentation of office processes, such as:
  - Patient sign-in sheets that ask for only minimal information.
  - Physical placement of computers running EHR so they can't be viewed by other patients, vendors, or other unauthorized individuals.
  - Mandating that employees lock their computers whenever they leave—even for a short period.
  - Procedures for the handling and destruction of paper records.
  - Management and storage of patient photographs if they are part of the patient record. Note that The Joint Commission strongly advises obtaining an informed consent to photograph.
  - Policies detailing which devices are allowed to contain PHI and under what circumstances those devices may leave the office.
- Encryption of all devices that contain PHI (laptops, desktops, thumb drives, and centralized storage devices). Make sure thumb drives are encrypted and the encryption code is not inscribed on, or included with, the thumb drive.
- Training your staff on how to protect PHI. This includes not only making sure policies and procedures are HIPAA-compliant, but also instructing staff not to openly discuss patient PHI.

- Audit and test your physical and electronic security policies and procedures regularly, including what steps to take in case of a breach. The OCR audits entities that have had a breach, as well as those that have not. The OCR will check if you have procedures in place in case of a breach. Taking the proper steps in the event of a breach may help you avoid a fine.

CASE EXAMPLE

A thief impersonating a construction worker stole a laptop after gaining access to a physician's office during a hospital expansion. The laptop was unencrypted and contained pediatric patients' names, treatment information, and diagnoses as part of a research study. An OCR investigation lasted four years before it was dismissed.

CASE EXAMPLE

A hospital lost unencrypted backup tapes during a remodeling project in its IT department. The tapes contained the information of 1.6 million pediatric patients, including names, Social Security numbers, dates of birth, diagnosis codes, and health insurance information. The tapes also included the information of 200,000 employees, physicians, and vendors. After more than 3 years, the OCR dismissed its investigation.

THWART RANSOMWARE ATTACKS

An employee opens an e-mail that purports to be from her bank and asks her to click on a link to her account. Instead, the link downloads ransomware, a type of computer virus that restricts access to the infected computer system and demands that the organization pay a ransom to the hackers. Some forms of ransomware, such as CryptoLocker, systematically encrypt files, making them impossible to decrypt without paying the ransom for the encryption key.

CryptoLocker propagates via e-mail attachments. When the attachment is opened, the virus encrypts the hard drive on the local computer and any mounted network drives. The virus then displays a message that offers to decrypt the data if a payment is made by a stated deadline through either bitcoin (see inset) or a prepaid cash voucher.

If the organization has performed frequent system backups, it can typically restore its data with limited loss. However, if backups have not been performed, the ransom must be paid or the organization must reset its system back to its default setting—and lose everything.

Ransoms are typically small enough that the FBI won't expend its resources to identify and prosecute the hackers, but some ransoms have been in the tens of thousands.

Also, under guidance released in July 2016, the Department of Health and Human Services now presumes that a ransomware attack compromises electronic PHI—unless the HIPAA-covered entity can demonstrate otherwise. The burden of proof rests with the healthcare practice. Small practices without sophisticated systems or firewalls may have to hire a forensic computer firm to demonstrate that a breach did not occur.

WHAT IS BITCOIN?

Bitcoin is a decentralized network that allows people to make online payments using bitcoin currency. The network has become popular because 1) it operates beyond the control of a government or bank, 2) its fees are lower than traditional payment networks such as credit cards, and 3) its transactions are anonymous. An individual can transfer bitcoin from his or her virtual bank account directly to another account using a computer or mobile app. A public ledger records all bitcoin transactions but reveals only account IDs, not names, making transactions untraceable. The operators of specialized computer hardware generate, or "mine," new bitcoin as a reward for solving complex math problems that enable the verification of bitcoin transactions. Existing bitcoin can be bought and sold on bitcoin exchanges using U.S. dollars, euros, and other traditional currencies.

⚠ To mitigate this risk, your practice should take these steps:

- Small practices should migrate their systems—both software applications and data—to the cloud. Cloud vendors have implemented security measures that most smaller practices won't be able to implement and maintain. Be sure to fully vet your cloud storage vendor (see page 8 of this guide for strategies on vendor selection).
- If you cannot store data in the cloud, consider working with a computer forensic firm to strengthen your security and investigate capabilities. Ensure that critical systems and business data are backed up hourly, and test that the backup restore process works.
- Provide ongoing security awareness for all employees. Over 80 percent of attacks occur due to human error or human involvement. Train staff members to avoid downloading files, clicking on links, or running unknown USBs on computer systems.
- Block malware by using intelligent firewalls to stop the software execution.

- Install intrusion-detection software to monitor illegal activities on computer networks.
- Stop malware from executing on desktop computers by installing application whitelisting software, anti-virus, or anti-malware.
- Perform penetration testing on a regular basis to determine any existing vulnerabilities that should be patched.
- Install software updates/patches regularly. These include patches that fix vulnerabilities in the software, helping support your antivirus software, your firewall, and all other security measures.

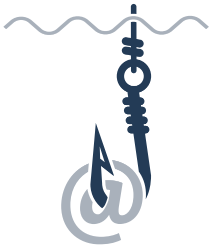
CASE EXAMPLE

A medical center suffered a ransomware attack that blocked access to its computer system. The center paid the equivalent of $17,000 in bitcoin to the hackers responsible, deciding that paying the ransom was the best way to restore normal operations. Ten days after the disruption was first noticed, the computer system was functioning again.

CASE EXAMPLE

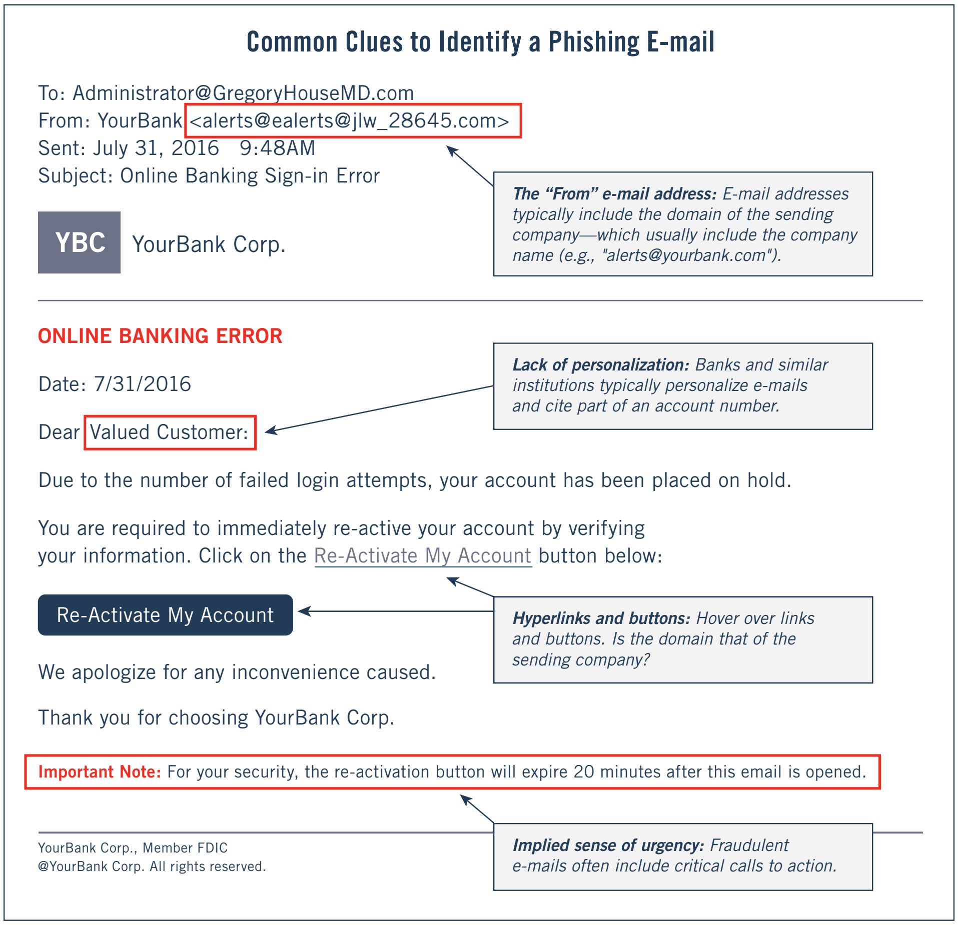
A ransomware attack affected 4 of the 9,800 computers in a hospital's network, making the information on the computers inaccessible. Because the hospital had saved critical data on servers instead of desktop computers, it avoided paying a ransom and prevented the loss of patient information. The hospital was able to find the virus, isolate it before it spread, and wipe the drives clean on the infected computers.

PREVENT SPEAR PHISHING



A common method of stealing data is spear phishing, an e-mail designed to lure recipients into providing personal information and clicking on malicious links.

Attackers often use stolen information to create these e-mails, or they use information available via Google and social networking sites. Unfortunately, these spear phishing e-mails seem plausible to some victims.



Common Clues to Identify a Phishing E-mail

To: Administrator@GregoryHouseMD.com
From: YourBank <alerts@ealerts@jlw_28645.com>
Sent: July 31, 2016 9:48AM
Subject: Online Banking Sign-in Error

The "From" e-mail address: *E-mail addresses typically include the domain of the sending company—which usually include the company name (e.g., "alerts@yourbank.com").*

YBC YourBank Corp.

ONLINE BANKING ERROR

Date: 7/31/2016

Dear Valued Customer:

Lack of personalization: *Banks and similar institutions typically personalize e-mails and cite part of an account number.*

Due to the number of failed login attempts, your account has been placed on hold.

You are required to immediately re-active your account by verifying your information. Click on the Re-Activate My Account button below:

Re-Activate My Account

Hyperlinks and buttons: *Hover over links and buttons. Is the domain that of the sending company?*

We apologize for any inconvenience caused.

Thank you for choosing YourBank Corp.

Important Note: For your security, the re-activation button will expire 20 minutes after this email is opened.

Implied sense of urgency: *Fraudulent e-mails often include critical calls to action.*

YourBank Corp., Member FDIC
@YourBank Corp. All rights reserved.

⚠ To avoid this risk, your practice should train employees to take these steps with every e-mail:

- Stop multi-tasking and pay attention to the e-mail.
- Preview the e-mail content thoroughly.
- Be suspicious if the e-mail asks you to click on a link or open an attachment, if the e-mail is from a sender you don't know, or if the e-mail comes from someone you know but contains a generic message (e.g., "Check this out" or "Thought you'd be interested in this").

- Exercise caution with any e-mail that includes a critical call to action (e.g., "Your account will be closed if you do not respond within the next hour").
- Ask the following:
  - Have I ever received anything like this before from the sender?
  - Does the e-mail appear professional, grammatically correct, and on topic?
  - Am I expecting hyperlinks or attachments?
  - If I hover my mouse over a link, is the URL authentic?
  - Can I access the information another way?

If the answer to any of these questions is "no," call the sender to verify the message is genuine. If not, delete the e-mail.

CASE EXAMPLE

The OCR launched an investigation after a sophisticated foreign spear phishing attack exposed the information of nearly 20,000 pediatric patients. Healthcare employees clicked on phishing e-mails and either gave up credentials or launched malware into their network. The data contained patients' names, clinical information, addresses, phone numbers, insurance information, and some Social Security numbers.

COMBAT PASSWORD THEFT

Hackers can gain access to your data by capturing or guessing the passwords used by your employees. Despite warnings about the dangers of easily identifiable passwords, many people still use birthdates, children's names, other personal information, or even sequential numbers ("12345678").

⚠ To reduce this risk, train employees to do the following:

- Avoid using the same password for multiple accounts.
- Don't use a variation of a prior password when creating a new one (e.g., "FuzzyDog1," "FuzzyDog2," "FuzzyDog3," etc.).
- Avoid simple words found in the dictionary. Hackers use sophisticated programs that crack passwords.
- Don't use names or things that could be identified from your social networking accounts (your pet's name, children's names, hobbies, anniversaries, alma mater, etc.)
- Memorize passwords. If a password must be written down, only write one portion and commit the other portion to memory.

- Consider using pass phrases of at least eight characters instead of passwords. Pass phrases are easier for users to remember, yet more difficult for hackers to decode (e.g., “81PurpleBagels!” for graduation year, favorite color, and favorite food).
- Intentionally misspell words (“Greeen” instead of “Green” or “Datte” instead of “Date”).
- Use both uppercase and lowercase letters (“GreEn” or “DaTe”).
- Use special characters (“Green!”). Some sites restrict what special characters can be used, but use them whenever possible. Cracking programs know common letter replacements, so avoid the obvious ($ for S, 3 for E, 1 for I).
- Combine words, special characters, and numbers (“GreEn!1920”).

To further reduce your risk, consider the following system controls:

- Require that passwords be updated every 90 to 120 days.
- Lock users out after three failed login attempts and allow only an administrator to restore access.
- Limit EHR accessibility with user authentication/credentialing (e.g., user id and password).

Your practice can also use a password database, a program that allows an employee to establish a master password that manages all other passwords. Many password databases can be downloaded as a plugin for common web browsers. Though one vulnerability is the risk of a hacker discovering a master password, thereby exposing the entire network, a password database is generally the most secure way to prevent compromised passwords.

SCRUTINIZE YOUR VENDORS

Even if your practice has systems in place to prevent the likelihood of a cyberattack, your patients’ information can still be exposed as a result of an attack on one of your vendors.

Examples include transcription firms and medical billing processors, or even a law firm or CPA. Many physicians and practice leaders may assume that if the vendor suffered the breach, then the vendor is responsible for notifying your patients. However, in those cases, the practice is still responsible for notifying patients of any disclosure. This is because the practice performs and owns the initial intake of information.

To mitigate this risk, adopt the following practices:

- Carefully audit any vendor that will handle your patients' data.
- Ensure your vendors understand and are addressing privacy concerns.
- Require a confidentiality agreement for all vendors. This agreement should focus on vendor confidentiality obligation, compliance with the law, reporting of breaches, and reimbursement for any damages caused by the vendor's negligence.
- Ask detailed questions about each potential vendor's systems, and monitor each vendor's privacy efforts.
- Carefully evaluate and monitor the way you securely encrypt transmission of data to your vendors.

CASE EXAMPLE

A hospital's IT vendor inadvertently unsecured a file containing the information of over 30,000 patients, making the data publicly accessible via Google and other search engines. The hospital discovered the incident during security testing after a larger system acquired it. The exposed information included patients' names, Social Security numbers, dates of birth, addresses, treatment information, and insurance information. In response, the hospital hired services that included legal, forensics, call center, credit monitoring, and crisis management. The OCR and four attorneys general investigated the incident.

KEEP CLOUD DATA SAFE

Healthcare practices and facilities are depending more and more on cloud storage because it gives users the ability to access data across a variety of electronic devices while eliminating the costs and difficulties associated with maintaining a physical storage system. This makes cloud storage particularly useful for small practices.

Cloud storage is a network of remote servers that allow for centralized data storage and online access to these resources. Your files are stored on a server connected to the Internet instead of being stored on your own computer's hard drive or data center. This eliminates the need to purchase hardware equipment to store files or to upgrade your hardware to get extra storage space—or the need to delete old files to make room for new ones. The cloud is convenient and cost-effective, providing a way to automatically back up your files and folders.

The cloud can be a safe and appropriate method of data storage, but the safety level of the cloud, and whether it's appropriate for use, depends on the vendor.

⚠ The decision to use the cloud to store HIPAA-protected records should not be made until substantial due diligence has been performed on the cloud service provider. Keep the following issues in mind:

- Are the vendor's security standards appropriate? Make sure the company has a good reputation and solid security policies. You are entrusting the provider to store your information, so the extra time spent researching and comparing providers and their security practices will pay off in the long run.
- How much data will you be storing? Many companies charge by the amount of storage you use, so understand what your needs are before choosing a vendor. Ensure the vendor can handle the amount of data you would like to move to the cloud.
- Ensure your data is encrypted when being uploaded to or downloaded from the cloud. This is also your responsibility. Make sure your browser or app requires an encrypted connection before you upload or download your data. Also ensure all devices that contain PHI are encrypted.
- Most importantly, make sure your HIPAA-protected data is encrypted when stored in the cloud. Data protected by law, such as medical information or personal identifiers, should never be stored in the cloud unless the storage solution is encrypted. Many cloud service providers store data on a cloud server with no encryption, meaning anyone who has (or can get) high-level access to that server will be able to read your files. Carefully review the specific terms of service within your agreement with the provider to ensure it guarantees encryption of all of your stored data.
- Select which members of your organization will be able to decrypt the data, and create policies detailing under what circumstances information can be decrypted.
- Understand how access is shared in your cloud folder. Many cloud storage providers allow you to share access to your online folders. Be familiar with the details on how that sharing works. Is access read-only or can the user edit the file? Can you identify the last person to edit a file? Awareness of who has access, and how access is gained, is critical to monitoring activity within your stored data.
- Understand your options if the cloud provider is hacked or your data is lost. Virtually all cloud service providers require a user to sign an agreement that contains a terms of service provision. In most cases, these agreements provide that the user has very little, if any, remedy if a hack or a loss of data occurs. Pay attention to what rights you have given up and make sure you are comfortable with that decision.

RESPOND APPROPRIATELY TO A BREACH

If you have a reasonable suspicion that your patients' data has been compromised, you are legally required to investigate. If a breach is found, you are then required to notify affected patients. The investigation and notification process is generally lengthy and complex, and cumulative costs for these requirements are likely to be very high.

⚠ If you suspect your data has been breached, respond quickly with the following steps:

- Hire an attorney who is experienced in data breach law. Because this is an emerging specialty, it may be difficult to find a lawyer with this type of experience.
- Hire an IT forensics expert who can help identify the cause and possibly even the source of the breach.
- Once the legal and forensics reviews are underway, notify the affected individuals. Most laws require you to notify patients with letters sent through the U.S. Postal Service.
- Notification letters are likely to cause recipients to call for more information. In cases of large numbers of affected patients, hiring a call center may be the most efficient option. Call-center personnel are trained and can deliver a consistent message to callers.
- Finally, a standard industry response to a substantial breach is to provide a remedy to affected individuals, such as a credit-monitoring service.

PREPARE FOR LAWSUITS

To add further complication to an already difficult process for practices and patients, trial attorneys are creating a new niche for themselves: data breach class actions.

Large data breaches are often associated with expensive litigation and settlements, and a growing number of attorneys are now prospecting for well-publicized breaches. These attorneys will aggregate a class of affected individuals to sue providers for statutory damages, citing laws created well before the rise of cyberattacks. Though only a small number of these lawsuits have made it to court, providers who are sued must still defend themselves.

Be sure to enact an effective, quick response once you experience a breach. The trial attorneys will endeavor to discredit your response to build their case.

As discussed earlier, state or federal regulatory agencies are likely to investigate substantial, well-publicized breaches. The OCR is a well-staffed, well-funded agency that likes to make examples of organizations that do not adequately protect the personal information of their patients. Fines are possible, and the damage to your reputation can linger for years.

CASE EXAMPLE

A hospital employee stole patient information and sold it to a local crime ring, who filed fraudulent tax returns. Law enforcement informed the hospital, which began an investigation and notified the 115,000 affected patients. The OCR launched an investigation and attorneys filed a class action, though it was ultimately dismissed.

CASE EXAMPLE

Seven class actions and an OCR investigation resulted after thieves stole two unencrypted desktop computers from an office building. The computers contained the master patient index for the physician group of a healthcare organization of four million patients.

PLAN YOUR RESPONSE NOW

The single most important element in preventing or minimizing a data breach is to develop and implement an Incident Response Plan (IRP). An IRP will vastly improve the timeliness of your response to a breach. Regulators and trial lawyers will look very closely at your response, so acting sensibly and having a strategic, structured plan in place makes all the difference in the world. In the heat of the moment, you do not want to scramble and improvise.

⚠ To prepare a strategic breach response, build an IRP that contains these three elements:

- Adopt robust system controls, especially encryption for laptops and mobile devices. Some of the largest breaches have occurred because of lost or stolen laptops or smartphones. Encrypting the data on these devices ensures safe harbor. Most state laws concerning breaches have safe harbor provisions for organizations that encrypt data. Be aware that password protection is not encryption.
- Train staff to reduce your exposure to breaches. The goal is to protect information and patients and to help employees understand how to treat data. All trainings should be documented.
- Transfer risk. Insurers are offering more products that directly address data breach risk and will help cover many of the costs you'll incur when you investigate and respond to a breach. It's important to have the right coverage built into your overall risk management plan.

SUMMARY

It is impossible for even the best prepared practice to be immune from the threat of a cyberattack or data breach. New risks are always emerging. However, taking the steps outlined in this guide—while not exhaustive—can greatly improve your defenses.

Start by training staff members on how they can protect PHI, identify malicious e-mails, and avoid password theft—these measures alone can go a long way toward mitigating your risk. Then implement needed technologies such as system backups, firewalls, software updates, and password managers. Once you've put these preventative measures in place, organize your data breach response. Your vigilance can have a direct impact on the likelihood of a breach and can minimize a breach's effects on your patients and your practice.

PROTECTING PRACTICES AGAINST EMERGING RISKS IS JUST ONE WAY WE'RE TAKING THE MAL OUT OF MALPRACTICE INSURANCE.

Founded and led by physicians, The Doctors Company is relentlessly committed to advancing, protecting, and rewarding the practice of good medicine. The Doctors Company partners with practices of all sizes to help them manage the complexities of today's healthcare environment by providing expert guidance, resources, and coverage. The Doctors Company is the nation's largest physician-owned medical malpractice insurer, with 79,000 members and over $4 billion in assets, and is rated A by A.M. Best Company and Fitch Ratings

An industry thought leader in risk management, The Doctors Company helps healthcare practices understand and mitigate liabilities, so they can focus on doing what they do best—delivering superior care.

CyberGuard®, part of The Doctors Company's medical liability policy, covers the costs of investigating and responding to a cybersecurity breach, including the cost of data recovery, patient notification costs, and network asset protection. Make sure you're protected from this serious exposure—learn more at **thedoctors.com/cyberguard.**

CONTRIBUTORS

David McHale, Senior Vice President, General Counsel, The Doctors Company.
Craig Musgrave, Senior Vice President, Chief Information Officer, The Doctors Company.
Paul G. Nikhinson, Esq., CIPP/US, CIPP/E, Beazley Breach Response.

[1] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Ponemon Institute. May 2016.
[2] Ibid.

The guidelines suggested here are not rules, do not constitute legal advice, and do not act as a guarantee that a system breach will not occur if followed. The ultimate decision regarding the appropriateness of specific cybersecurity tactics must be made by each individual healthcare provider in light of all circumstances and in the healthcare provider's best judgment.

THE DOCTORS COMPANY
medical ~~mal~~practice insurance