The Tech chronicle

Inside This Issue

April 2023

This monthly publication provided courtesy of Patrick Birt, President of AdRem Systems Corporation.

Our Mission: AdRem is a company of respected, trusted, and proven individuals dedicated to delivering Today's innovative technologies for a more secure nation of tomorrow.

What Compliance Standards Does Your Business Need To Maintain?

Understanding HIPAA, NIST And CMMC

Compliance standards are some of the most important things a business needs to maintain to be profitable and well-respected while staying out of legal trouble. Failure to meet these standards will make your business susceptible to fines and legal action. You'll also take a hit on your reputation as customers, vendors and competitors may find your business to be untrustworthy. By enforcing compliance, you're working to promote ethical behavior while protecting the rights of your employees, customers and other stakeholders.

But it's not always obvious which compliance standards apply to your industry or specific business. While most businesses need to ensure they're following Occupational Safety and Health Administration standards for workplace safety, they must also meet Environmental Protection Agency regulations for protecting the environment. There are also compliance requirements that have to do with the information you store and share. Here are three other compliance standards that you should know about if you're a business owner or leader.

Health Insurance Portability And Accountability Act (HIPAA)
You probably already know about HIPAA if you've been to any doctor's appointment in the past two decades. This law was enacted in 1996 to protect the privacy of individuals' personal health information and to ensure the security of that information. HIPAA only applies to "covered entities," which include health care providers, health plans and health care clearinghouses. These entities must comply with the rules set forth by HIPAA when handling protected health information. They must have the necessary administrative, technical and physical safeguards in place to ensure the confidentiality, integrity and availability of the information.

Continued on pg.2

Continued from pg.1

There's been confusion in the past relating to HIPAA, especially during the Covid-19 pandemic. When employers requested vaccination status from their employees, many claimed that this violated HIPAA, which is false. HIPAA only applies to covered entities. It's essential that you know the ins and outs of HIPAA if you work in the health care industry. Noncompliance can lead to fines, legal trouble and, in some cases, the loss of your license to practice medicine.

National Institute Of Standards And Technology (NIST)

The NIST is a nonregulatory agency of the United States Department of Commerce that develops and promotes standards, guidelines and best practices for ensuring the security and privacy of information systems. NIST compliance is vital for any organization that handles sensitive information, such as personal data, financial information or intellectual property. It becomes even more important for heavily regulated industries like health care, finance and government. NIST compliance can help organizations protect against cyberthreats, data breaches and other security incidents. It also helps organizations meet regulatory requirements set by HIPAA.

> **"By enforcing compliance, you're working to promote ethical behavior while protecting the rights of your employees, customers and other stakeholders."**

When you adhere to NIST standards, you'll easily identify vulnerabilities, improve incident response plans and prioritize security measures. The NIST has created a helpful framework and various publications that provide guidelines for various systems and scenarios. If you're looking for a specific publication or are interested in other NIST resources, head to their website, NIST.gov, for more information.

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a framework developed by the U.S. Department of Defense to assess and certify the cyber security practices of organizations that work with the DoD. This framework includes a set of controls and processes that organizations must implement to protect sensitive information and systems from cyberthreats. The CMMC framework applies to all organizations that work with the DoD and handle Controlled Unclassified Information. This often includes defense contractors, suppliers, subcontractors and organizations that provide services to the DoD, such as IT, logistics and engineering. Businesses that support the defense supply chain, including manufacturers, technology firms and professional service providers, also need to adhere to CMMC guidelines. Failure to achieve CMMC certification can result in being unable to bid on or win DoD contracts.

Compliance is something every business needs to be aware of, regardless of industry. Start by investigating HIPAA, NIST, and CMMC to see if their rules and regulations are applicable to your business, then look to other organizations. Doing so will help set your business up for success.

Free Download: The 9 Security Elements Of The FTC Rule. How Many Have You Implemented?

Are you aware of the new FTC Safeguard regulations coming into effect June 9th, 2023? You might ask yourself, why you should care. The FTC Rule clearly identifies the category of entities that are now considered financial institutions, including: a retailer that extends credit to consumers, motor vehicle dealers, property/real estate appraiser, mortgage brokers, credit counselors, accountants/tax preparation services, and many more.

The Safeguards Rule requires covered institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

Businesses Covered By The Safeguards Rule Must Comply With Provisions by June 9, 2023

Our 100% FREE download includes nine security elements your company's security program must include to be compliant with these new provisions. Use the form to provide a no risk IT security assessment of your system. Afterward, we'll provide you with recommendations. For a limited time, we are waving our IT assessment fee. That's right, we will give you a 100% FREE IT Systems Assessment and review the form with you.!

Get out ahead of this coming regulation and work with us to ensure your establishment is in compliance with the new FTC Safeguards Rule. *Download our form and Reserve your slot now!*

Download our Checklist and Reserve your Free IT Assessment
at www.AdRem.com/ftc-safeguards/

HIPAA Do's and Don'ts For Employers

The Health Insurance Portability and Accountability Act (HIPAA) applies to medical providers, insurance companies, and business associates of all sizes. The massive scope of the law and its requirements to fully comply with all parts means there is no "one size fits all" plan for HIPAA compliance.

However, some suggestions apply to organizations of any size and the employees who work for them. Here is a few HIPAA do's and don'ts for employers and employees.

HIPAA Do's for Employers

When thinking about HIPAA compliance, the most important thing to remember is that it's ultimately all about patients' protected health information (PHI). That is literally why the law was written– to provide standards for protecting the privacy and security of PHI in physical and electronic (ePHI) formats and to guarantee that patients have a right to access their own PHI. Here are three HIPAA do's for employers to remember:

DO a Security Risk Assessment (SRA) Annually

The first reason to conduct an SRA annually is that the law requires it to be done regularly, and best practice standards have defined "regularly" to mean once per year. Covered entities like healthcare providers and insurance companies must complete six individual audits as part of a complete SRA, including:

- The Asset & Device audit
- The IT Risk Analysis Questionnaire
- The Physical Site Audit
- The Security Standards Audit
- The Privacy Standards Audit
- HITECH Subtitle D Privacy Audit

Business Associates that must take possession of PHI to provide services for covered entities can skip the Privacy Standards audit, but they must complete the other five.

The second reason to complete an SRA annually is that it gives an organization a snapshot of where there may be gaps that could leave PHI vulnerable. Identifying these gaps and creating plans to eliminate them is good for patients and wise for your organization. Failure to complete a security risk assessment is one of the most common violations found in HIPAA audits.

DO Document Everything

If you have done everything required to fulfill every part of the HIPAA rules and regulations, you will still fail a HIPAA audit if you can't prove you've done it. That means keeping a record of all SRAs, gap remediations, HIPAA policies, employee training and attestations, business associate agreements, and possible breach incidents. It also means updating these items as needed and documenting those changes when they occur. HIPAA's attitude is that if you can't prove it, it never happened. So make sure you can prove it.

DO Respond to HIPAA Right of Access Requests Promptly

Under HIPAA, when a patient makes a written request for their medical records to a healthcare provider or insurance company, the covered entity has 30 days to respond. Even if they are "difficult" patients, and even if they have outstanding balances on accounts, a healthcare provider must provide the records in a timely manner.

The HIPAA Privacy Rule considers patient records held by a doctor to be patient property. There is no justifiable reason to refuse to grant a patient right of access request. HIPAA auditors with the Office for Civil Rights (OCR) have made right of access enforcement a priority, resulting in 41 fines and settlements in the past three years. In the last 14 cases, the average HIPAA fine for violations was

Continued on pg.4

Continued from pg.3

$55,785.

HIPAA Don’ts for Employers

While there are many things employers shouldn’t do when it comes to HIPAA compliance, there are a few that stand out:

DON’T Allow Employees to Share Passwords

This activity undermines your ability to comply with two major provisions of HIPAA–the HIPAA Privacy Rule and the HIPAA Security Rule. The HIPAA Privacy Rule defines standards for protecting the privacy of patient PHI by limiting the unauthorized release of data. Unauthorized release to individuals outside your practice is a blatant violation of this rule.

But the Privacy Rule also applies to users inside your organization. The HIPAA minimum necessary standard states that users should only have access to the minimum amount of PHI needed to perform their jobs. That means billing clerks should not have access to a patient’s entire record, or nurses should not peek at records for patients they are not responsible for treating. If employees share passwords, you cannot control access to patient records.

Because sharing passwords violates widely-accepted practices for data security, it would also violate the standards of the HIPAA Security Rule. Simply put, don’t share password.

Don’t Ignore the Office for Civil Rights

As we mentioned earlier, OCR is responsible for enforcing HIPAA. Their investigations can be triggered by breach notifications, random audits, or by patient complaints.

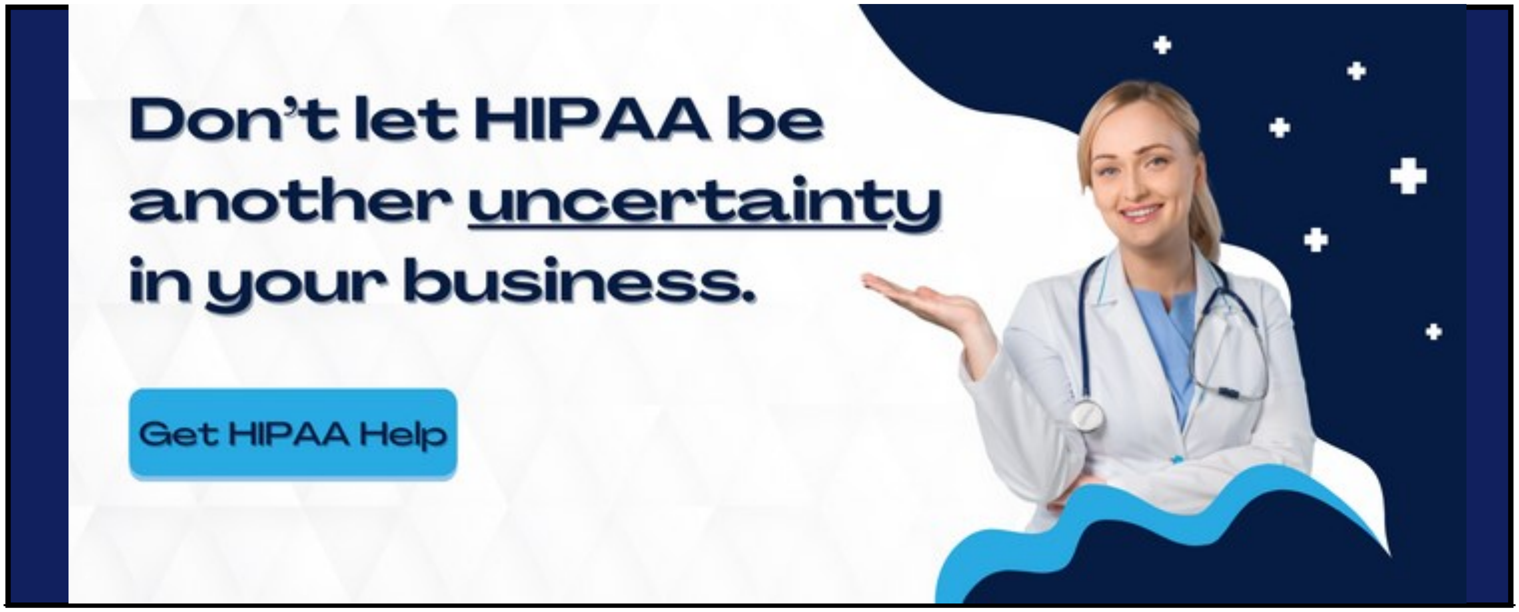
If OCR contacts you, the worst thing you can do is ignore them. In the past year alone, there have been at least two instances of doctors ignoring multiple requests for information from OCR auditors concerning right of access complaints.

As a result, each doctor was fined $100,000 for the violations. By comparison, a mental health practice responded quickly and received a $3,500 penalty.

The choice is yours. OCR auditors will not go away if you ignore them. Doing so will cost you in the long run.

One Final HIPAA Don’t: Don’t Go it Alone

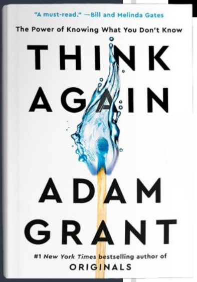
94% of healthcare organizations FAIL their audit because they did not have an effective compliance program in place. Find experienced professionals that know the specialties of HIPAA Compliance that can simplify the process and fulfill every requirement of the Law. AdRem’s team Partners with Professionals who have nearly 20 years of experience in helping medical professionals from all specialties navigate HIPAA compliance and help cure that HIPAA Headache.



Think Again

By Adam Grant

Many business leaders and entrepreneurs fall into the dangerous trap of overconfidence. They think they know better than others and are unwilling to change their mind. Think Again is a thought-provoking book that challenges readers to question their assumptions and consider alternative perspectives. Written by Adam Grant, a renowned organizational psychologist, Think Again is a powerful tool for expanding your critical thinking skills. Grant uses research, case studies and personal anecdotes to illustrate the importance of being willing to change your mind. Think Again is an excellent read for anyone in a leadership position, as it will help you make better decisions that will benefit your business.


"A must-read." —Bill and Melinda Gates
The Power of Knowing What You Don't Know
THINK AGAIN
ADAM GRANT
#1 New York Times bestselling author of ORIGINALS

Build a Brand Your Customers Will Love

There are many critical decisions business owners make that have the potential to bring customers in or send them away. Sometimes, it's difficult to know precisely what you need to do to attract your target audience, but there are a few tactics that provide promising results. First, you need to identify your core values and mission. Why are you in business and what separates you from the competition? Share your values and mission with the public through social media and your website once they are built. You also need to keep customer satisfaction at the forefront of your mind. Everything you do should encourage customers to return to your business. And finally, be transparent about your practices. Customers do not like to be left in the dark when things change.

Impress Any CEO In 3 Easy Steps

You have a meeting scheduled with a CEO. Your goal is to convince them to either spend $1 million on your product or service, hire you or invest in your idea. What's your strategy?

Many people "show up and throw up" and push a lot of information at the CEO, either verbally or by PowerPoint. A CEO will not hire you simply because you show that you know what you're talking about. Another flawed approach is to phrase your request as a "we ought to." CEOs don't decide to do things just because other people say they should do something. Worse yet is when people only talk about why they want something to happen, ignoring the CEO's wishes, concerns and perspective.

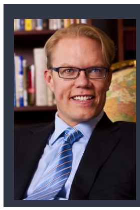
So, how do you successfully convince a CEO?

1. **Seek first to understand the CEO's perspective.** That is Stephen Covey's advice. It needs no further explanation. Your first step in discussing a topic with a CEO is to put all your energy into asking probing questions, listening and learning what the CEO thinks about a topic and why. Forget about your agenda or your needs for a moment.

2. **Reflect the CEO's perspective to their satisfaction.** This step is tricky. Most people cannot objectively reflect or restate another person's perspective about a topic without putting their own slant on it. I first learned this step during my psychology Ph.D. training during a class on conflict resolution. At this step, you must restate the CEO's perspective on the topic, simply and without putting words in their mouth or trying to spin it in your favor. You know you have succeeded once the CEO says the magic word, "exactly." This means that the CEO believes you understand their perspective. Then, and only then, have you earned permission to move to the final step.

3. **Propose your idea as a way to help the CEO achieve their goals.** The mindset for this step is not that you are about to trick or fool a CEO into doing something that's not good for them. Your mindset is that you are about to convince a CEO to do something that *is* good for them. (And by the way, if what you are about to propose is not in the CEO's best interests, then don't propose it!) A simple way to present your idea is to say, "Your goals are X, your concerns are Y, so I propose you do Z."

Contrary to popular belief, great ideas don't sell themselves. It takes a skillful leader to successfully convince a CEO, and now you have the tools to do so.



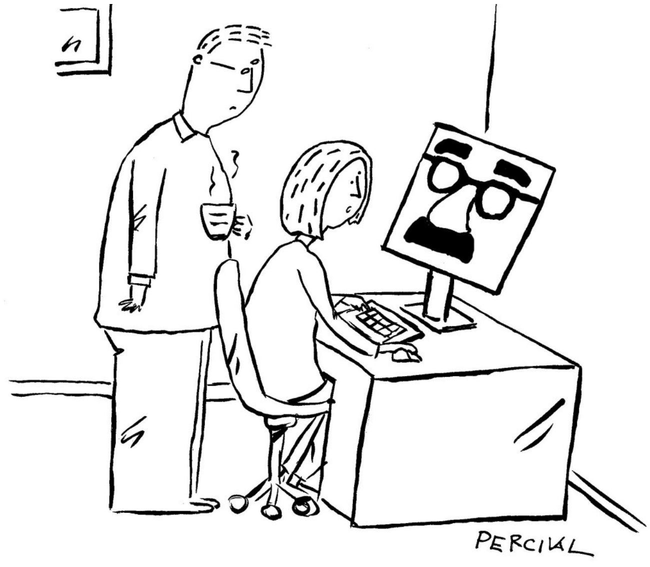
Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *bestsellers. He stays active in his community and has advised many government officials.*

Are You Addicted To Work? 2 Ways To Help Take Your Life Back

Many business owners and entrepreneurs will dedicate their entire lives to their businesses to ensure success. They'll regularly work 60- to 80-hour workweeks, sacrificing their free time to focus on their business. In many ways, it's an addiction that can be incredibly damaging to an individual's mental health. Recent studies have shown that those who work too much are more susceptible to burnout, chronic stress and strained relationships. If you find yourself spending too much time in your business, there are a few things you can do to fight your work addiction.

Reassess Your Goals.
Why are you working so hard? What do you want to achieve? Is it actually possible, or are you working yourself into the ground for an unobtainable dream? These are questions you need to ask yourself if you feel you're working too much. Reflect on your goals and determine if they're still what you want for yourself and the business. If not, or if your goals are not feasible, it's time to readjust and create new ones.

Trim Your Task List.
Working too long every day usually stems from trying to accomplish too much daily. Take a step back and think about what you can truly accomplish in 8–10 hours. Don't put too much on your plate because you'll feel like you need to complete everything before you head home. Delegate the less important tasks if you have a team supporting you. You don't have to do everything in one day on your own.



"The computer's acting funny."

Why Aren't My Employees Reading My E-mails?

How often do you send out e-mails to your employees? Have you ever talked with an employee about prior communication you sent, but they tripped their way through the conversation? It happens all the time across various industries. Employees don't always read communications from upper management, and you're left trying to figure out why. Sure, you could blame it on the employees just not wanting to read, but there's often a deeper issue involved. Here are a few reasons your employees are ignoring your e-mails.

- **Improper Timing:** Your employees are less likely to read your e-mails if you send them out at the end of the day.
- **Information Overload:** E-mails with too much information cause your employees to take too much time from their other tasks. Only put the information that's absolutely necessary in your e-mails.
- **Unclear Expectations**: Are your employees required to read your e-mails? They might just ignore the e-mails if they don't think they pertain to their job or provide relevant information.