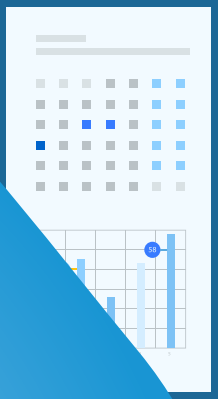
a COUPLE of GURUS™



THE HIPAA ROADMAP

for Medical Device Manufacturers

Transform your biggest headaches into stress-free checkups

THE HIPAA ROADMAP

for Medical Device Manufacturers

TABLE OF CONTENTS

THE TROUBLE WITH HIPAA

Even if you can't name a device manufacturer (MDM) that's been fined for violating the Health Insurance Portability and Accountability Act (HIPAA), you know these stories exist. Tales of a complicated and bureaucratic law that stifles entrepreneurship. But what if we told you that most HIPAA breaches are far less sinister than hackers with sophisticated knowledge targeting a medtech business from afar?

In 2013, the largest medical device manufacturer in the world, Medtronic, lost a box of training records containing patient information. The company issued a statement that the box was "believed" to be somewhere in its Minnesota facility, but there was a possibility it had been stolen. Thankfully, a "very small number" of patients were affected according to Medtronic's press release...only 2,764.

Despite the simple oversights that lead to most HIPAA breaches, the majority of the law centers around IT-related countermeasures. That puts an unfair burden on small operations like MDMs.

The good news

Everyone agrees that HIPAA should protect patient health information (PHI), electronic or otherwise, without impeding business growth. If you don't have access to any patient information, you don't need to be compliant! Simple as that. But how can a regulated startup expect to achieve compliance if an organization like Medtronic, worth billions of dollars, couldn't avoid a breach?

In reality, smaller medical device manufacturers actually have an advantage. It's so much easier to integrate employee training, IT best practices, and high-tech solutions during the early stages of growth. It just takes a detailed plan and an experienced guide.

HIPAA: Countless routes to compliance

Like most regulatory frameworks, HIPAA doesn't provide black-and-white requirements for achieving compliance. One of the most clear cut pieces of advice from experts is to encrypt all the PHI you store, but even that isn't mandatory based on the text of the law.

HIPAA focuses on the ends rather than the means — if you can prove ***you've invested significant effort*** to keep your data safe, you've already done most of the heavy lifting.

Privacy rights

There is some specificity to fall back on. For example, a HIPAA-regulated business must obtain and retain written permission to disclose an individual's PHI outside of the business. Patients also have the right to request copies of all their information stored by regulated businesses.

Those requirements may sound simple enough, but the definition of PHI is broader than most MDMs realize. Letting someone outside of your organization know the name and phone number of a device user is enough to land you in hot water.

To achieve these standards, HIPAA requires that you nominate a Privacy Official to ensure that all PHI disclosures are cataloged. In the unfortunate case of a breach, the Privacy Official is responsible for notifying government entities and affected parties within certain timeframes.

Data security classifications

Every threat to the PHI you store falls into one of three categories: technical, physical, administrative. If you can understand these threats and put safeguards in place to prevent them, you'll never need to worry about failing a HIPAA audit:

- Technical safeguards protect you from the threats that ***exploit technology***. The WannaCry ransomware, for example, took advantage of a Windows bug that granted remote control over a targeted computer.
- Physical safeguards prevent data ***breaches related to hands-on access to data***. If front-desk employees leave their computers unlocked and unsupervised, a criminal with zero training could walk in and view, edit, or delete PHI records.
- Administrative safeguards are your ***policies and procedures for ensuring ongoing compliance***. When MDMs fail to regularly rehash employee training and revise their security policies, they leave themselves open to new and groundbreaking attacks.

Your compliance, your way

Ultimately, the simplest and most effective plan depends on the devices you manufacturer, how patients will use them, and your company's business associates. A good rule of thumb is this: If you take patient data security as seriously as you take the protection of your intellectual property — you're on the right track.

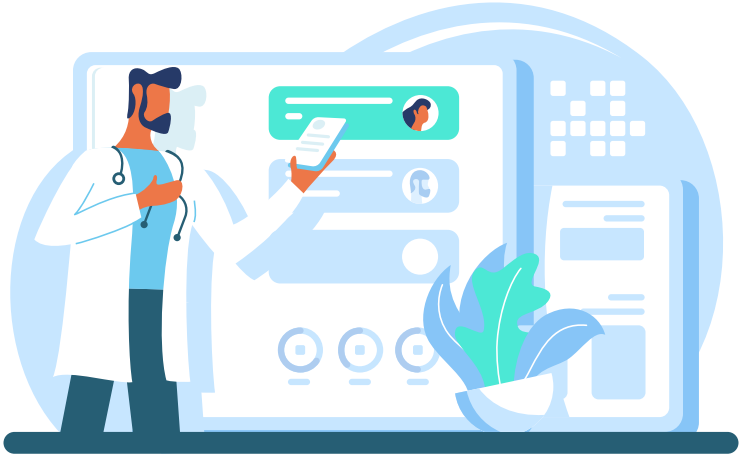
That probably sounds intimidating since most MDMs have thousands of PHI records and only a handful of prototypes. But don't worry. Like any long and complicated journey, everything is much easier with a plan.

SECURITY MILESTONES: Map out one year at a time

One reason that compliance efforts are so overwhelming for MDMs is that they're never truly finished. As time passes, your original employee training agendas will become less comprehensive and your technical safeguards won't be enough to prevent cutting-edge attacks. That's why we recommend sticking to a one-year plan.

After 365 days, hit the reset button and reevaluate your compliance plan as if you were just getting started. If you're lucky, most of your HIPAA efforts won't need to be updated. But the ones that will need to be refreshed could make all the difference during an audit.

Before getting started, appoint a Privacy Official and a Security Official to take ownership over each step in the process. The former takes care of the "people" tasks (employee training, PHI disclosure arrangements, etc.) while the latter takes care of everything else (IT solutions, physical security, etc.). Keep in mind that officials can be outside experts.



SECURITY MILESTONES: MAP OUT ONE YEAR AT A TIME

Here's what a one-year plan might look like for a Minnesota-based MDM:

STEP 1: Assess your technical safeguards (firewalls, antimalware, etc). Ideally, this is handled by someone with a fresh perspective and relevant certifications.

STEP 2: Install IT solutions to address gaps in security uncovered by your technical safeguards assessment.

STEP 3: Assess your physical safeguards, such as CCTV, keycard locks, etc. (only after finalizing new and upgraded technical safeguards).

STEP 4: Implement physical security measures to prevent risks uncovered by your physical safeguards assessment.

STEP 5: Catalog every vendor you work with that has access to your PHI in any way (e.g. outside accounting support).

STEP 6: Draft business associate agreements to ensure each one maintains strict security practices when handling your data.

STEP 7: Create a breach response plan (with steps for stemming additional damage and notifying affected parties).

STEP 8: Provide written guidance to ***all employees*** regarding all HIPAA-related requirements and data security expectations.

STEP 9: Conduct an all-company training event covering everything in steps 1-8. Simulated breaches and roleplaying are highly encouraged.

STEP 10: Assess your administrative safeguards (steps 5-9) and make updates where necessary.

STEP 11: Audit ***everything***. Revisit safeguards, policies, and procedures from each step to confirm that they haven't fallen behind in the interim.

STEP 12: Start the process over (or outsource the work to us!)

A big part of HIPAA compliance is documentation. If you have detailed logs of what was discovered and addressed during each step in the process, auditors will be far more lenient.

DEVICE-SPECIFIC HIPAA CONSIDERATIONS

Depending on the devices you manufacture, there may be several other concerns you need to address. For example, if devices are routinely returned to your facility for checkups or maintenance after collecting data, you should track each device's location and its handler at all times.

Additionally, some MDMs work with third-party vendors to fit their devices to end-user specifications. If these measurements have names, addresses, and other identifiable information associated with them — access should be locked down. Employees and vendors who don't need to handle devices or related data for their work should be prohibited from physical or technical access.

Another growing concern is whether or not devices can be wirelessly exploited. Because if an MDM sells pacemakers, implants for treating sleep apnea, or any other devices that send and receive data, the manufacturer could be liable in cases when that information is accessible to unauthorized parties. MDMs should be ready to address these concerns ***before*** going to market.

REGULATORY ROADBLOCKS: Learn from the mistakes of others

Our roadmap leaves a lot open to interpretation, but we can't get any more specific without understanding an MDM's unique needs. We can, however, highlight some common HIPAA compliance mistakes. Take a look at the following news stories and ask yourself: Could any of these breaches happen to me based on our current data security efforts?

REGULATORY ROADBLOCKS: LEARN FROM THE MISTAKES OF OTHERS

A shredded reputation

One well-meaning paralegal donated used paper from a Minneapolis-based law firm to her child's school. Students were using the scrap paper for classroom drawings until one parent pointed out the shocking PHI printed on the used side of the paper. The firm had a clear policy for shredding these records, but the paralegal simply forgot.

Free optimization (regulatory fine not included)

An IT contractor working for a Health and Human Services office in Maine uploaded over 2,000 names, addresses, and social security numbers to a free cloud service that reorganizes messy data. Are you sure that every app and service you use abides by rigorous security practices?

One expensive typo

A Cincinnati-based medical center accidentally emailed PHI to someone outside of the organization nine times because two letters had been swapped in the recipient's address. You could avoid a similar mistake simply by prohibiting access to internal documents to anyone from outside your organization — even if email attachments go to the wrong person.

Password: 'hipaaviolation'

The Utah Department of Health set up a test server and gave it a weak password, thinking that it wouldn't store anything important. Well, mistakes happen, and the server was given access to ***780,000 PHI records***. If technicians had enabled multifactor authentication, which requires more than one piece of identity verification (e.g. password plus a fingerprint, mobile SMS, or something else), even a password as absurd as '1234' would've prevented the breach.

App last updated 2003

An Anchorage-based mental health provider was fined $150,000 because of a malware attack that exposed 2,743 patient records. The culprit? Outdated software that was no longer receiving updates from the vendor created attack opportunities for hackers. That's scary considering the average business uses dozens of apps and has no idea when the last update was released.

THERE'S AN EASY WAY AND A HARD WAY

Device manufacturers that struggle with HIPAA compliance, no matter how unique their product, tend to run into the same issues. Imagine Entrepreneurial Erin runs a company that's working on a groundbreaking medical device. Her company has plenty of investment funds to bring their device to market but need to address compliance concerns before scaling up.

THE EASY WAY...	THE HARD WAY...
Erin contracts an established IT provider that specializes in compliance to set up, implement, and maintain the company's HIPAA efforts.	Erin asks her in-house IT guy to research what HIPAA requires.
The provider conducts a comprehensive technology assessment and presents a list of recommendations accompanied by a timeline and estimated budget.	The in-house technician spends a couple of weeks researching compliance requirements and comes back with a long list of confusing and contradictory recommendations.
Erin approves the provider's proposed plan and a team of experts get to work implementing the recommendations.	Lacking confidence in the technician's research, Erin decides to pay a consultant for a compliance plan.
The company's in-house IT guy focuses on day-to-day technical support while the provider maintains a laser focus on achieving compliance on time and on budget.	The in-house IT guy gets to work on the consultant's recommendations but everytime someone's computer freezes he has to put compliance efforts on hold.

THERE'S AN EASY WAY AND A HARD WAY

THE EASY WAY...	THE HARD WAY...
As part of its service, the outside provider works with Erin's technician to put together a company-wide compliance training event.	Still unsure of HIPAA's requirements, the technician asks Erin to bring the consultant back in to hold a company-wide compliance training event.
A few months after the compliance process began, Erin receives a finalized self-assessment that declares the company ready for a HIPAA audit.	About a year after the compliance process began, the IT guys attempts the company's first self-assessment. It's a bust when he realizes several employees and devices have been added to the mix without his knowledge. It takes weeks to make the necessary updates.
Hackers release a new type of cyberattack that was impossible to anticipate. Thankfully, the company's breach response plan is finalized and employees are trained on how to use it. Furthermore, the IT provider is still on the hook for emergency support. Losses were minimized, security upgrades were installed quickly, and compliance was reestablished.	Hackers release a new type of cyberattack that was impossible to anticipate. Employees implement the outdated response plan that doesn't account for new personnel and devices, which means the breach spreads further. Everything must be taken offline while the in-house technician quarantines and computers, accounts, and records one by one.
The company has HIPAA compliance in the bag and moves onto scaling up research and production. It's back to business as usual.	The technician is still juggling day-to-day support and finalizing compliance efforts. It's back to business as usual.

Secure and simplify your IT

In the short term, outsourcing HIPAA compliance means fewer technology headaches for you and your staff. In the long term, your company will be more valuable and attractive to investors.

A managed IT services provider (MSP) like A Couple of Gurus offers ongoing around-the-clock support — far more than a consultant can provide. What's more, MSPs never need to choose between day-to-day support and long-term HIPAA efforts. They can handle both in a fraction of the time that an in-house technician has available.

WANT TO LEARN ABOUT OUR HIPAA SOLUTIONS FOR MEDICAL DEVICE MANUFACTURERS?

Schedule a call with our experts today!

Phone: 612-454-4878 Email: info@acoupleofgurus.com

aCOUPLE of GURUS™

www.acoupleofgurus.com