HOW TO MASTER HIPAA COMPLIANCE

Some eat steak.
We eat software.

FAYE

fayedigital.com

IN THE HEALTHCARE COMMUNITY, DATA PRIVACY IS ESSENTIAL.

Patients need to be able to trust their healthcare providers with their more personal information. In turn, those healthcare providers need to be able to trust their vendors and partners to adhere to the strictest of confidences.

In the wrong hands, such as hackers and other criminals, medical data can cause incredible and permanent harm. As healthcare professionals, protecting this information is one of our most important responsibilities. Laws like the Health Insurance Portability and Accountability Act (HIPAA) of 1996 ensure that every patient record is protected to the highest standards across the entire medical field.

Whether you are a healthcare provider, manufacturer, distributor, or any other business working in the medical industry, you need to adhere to HIPAA Compliance.

IMPROVING HIPAA COMPLIANCE

While we all take this duty to protect patient data seriously, there's always room for improvement.

Utilize HIPAA Compliant Software

A great place to start with thinking about improving HIPAA compliance is to use tools equipped with the necessary requirements. With a HIPAA compliant Customer Relationship Management or Customer Experience software platform, you can transfer information quickly and safely, as well as leave notes directly into the patient file. This empowers you to focus on the patient experience without potentially sacrificing privacy.

Professionalize Your HIPAA Security

One of the biggest challenges faced by healthcare providers is ensuring that their systems remain compliant with HIPAA over time. As business practices and software systems change and update, there is always a risk — however small — that your office may become non-compliant or vulnerable to a data breach. Protecting your organization and patients may mean hiring a HIPAA security specialist, either as a consultant or as a member of your staff.

While your current staff may be able to effectively navigate the HIPAA requirements they face today, the specifics of the job will change over time. New technologies and updated systems will require examination by a skilled professional who is knowledgeable about HIPAA requirements. Even something as simple as a new CRM plugin could merit a HIPAA risk assessment.

Having a dedicated staffer to manage security needs, update policies, and conduct risk assessments may seem like a major expense, but the costs are miniscule when compared to the costs and fines that come as a result of a data breach. Depending on the size of your organization, you may even need a dedicated HIPAA Security Officer to ensure compliance.

Audit Systems

Every computer system has vulnerabilities. When those systems store valuable personal data, hackers and other criminals have major incentives to exploit those weaknesses. It's your organization's job to do everything possible to protect that data against every known threat. By regularly auditing your systems using the risk-assessment tools and checklists from the Office of Civil Rights (OCR), you can greatly reduce those risks.

The primary focus of these internal audits should always be the security of Protected Health Information (PHI). Even relatively simple security practices, such as positioning monitors displays with PHI away from public view and regularly updating passwords on your CRM and other databases, can have a huge impact on the overall security of your patient data. These audits should be done quarterly, with any failures addressed immediately.

Invest in Continuing HIPAA Training

Chances are that most of your staff see HIPAA compliance training as something between an understandable responsibility and a tedious chore. We all understand the importance of HIPAA rules for protecting our patients' privacy, but it's also easy for staff to lose focus of those rules over time. That's why it is essential to invest in continuing education and training, allowing your staff to remain sharp on their responsibilities.

Your organization's HIPAA training sessions should be an ongoing process, and it should also include any non-staffers and third-party vendors with access to sensitive patient data. It's essential that everyone involved fully understands the policies and rules they'll be expected to follow. These training sessions should also never be treated as a mere formality, and should be seen as an essential part of ongoing staff training.

Create a Comprehensive Breach Response Plan

Even the most cautious, well-prepared organizations can find themselves facing the worst-case scenario: An impermissible use or disclosure of protected patient data. While it's essential that your organization do everything it can to avoid a data breach, it's also important to have a plan in place well before a breach occurs. This means following the requirements established in HIPAA Breach Notification Rule (45 CFR §§ 164.400-414).

Under this rule, the individuals impacted by the breach must be contacted immediately, and informed about the specifics of the situation. If the breach is significant, impacting more than 500 people, both the office of the Secretary of Health and Human Services, and the media, must also be notified. And that's just the start of the process, well before the damage-control stage begins. Going into this kind of situation without a clearly defined plan is a nightmare for your entire organization. By investing in the creation of a breach response plan, your team can make even this nightmare scenario a little more manageable.

While you never want to plan for the worst-case scenarios, when it comes to patient data, it's of the utmost importance to be prepared. Creating a response plan is a proactive way to handle a breach, instead of a reactive way. Yet, there is more than one way to work to keep your data safe. Connecting your technology with compliance in mind can go a long way.

HOW TO CONNECT TECHNOLOGY AND COMPLIANCE

WE EAT
SOFTWARE

fayedigital.com

COMPLIANCE PROFESSIONALS HAVE ONE OF THE MOST THANKLESS ROLES IN ANY ORGANIZATION.

It's a job that almost sounds like it was invented as a punishment — creating reporting policies, training teams in regulatory requirements, conducting internal audits, and meeting with regulators — rather than being one of the most essential positions at any company. Compliance teams protect the company from costly and damaging regulatory fines and penalties. It's a job dedicated to managing risk.

It's also a job that isn't easily improved by new technologies. Regulations change all the time, as do companies' policies that respond to those changes. That's just not something that most software solutions are designed to manage. At the same time, properly incorporating compliance tools into a company's existing technology solutions is often worth the investment, as it results in both reduced regulatory risk and decreased costs.

To reap the benefits of connecting technology and compliance, off-the-shelf solutions simply aren't a viable option. These solutions need to be designed for specific regulatory requirements — HIPAA, for instance — while also fitting the unique use case of the business itself. It's a balancing act. Get it wrong, and it makes the compliance team's job even harder to do.

Focus on Efficiency

Compliance work is often labor intensive, requiring careful analysis of new regulations, policies, bylaws, and reporting protocols. It's a process driven by discussion and research, and that's not something that can be meaningfully improved by technology. What can be improved, however, is the compliance team's access to important data, reporting tools, and communication resources. Information silos can be broken down, and information can be centralized for easy access. This concept is important for disclosure management, auditing transparency, compliance monitoring, and document collaboration.

Use Technology to Force Compliance

One of the ongoing headaches for any compliance officer is making sure that everyone follows the rules. By building compliance checks into the CRM or other business tools, it's possible to simply stop progress on a given task until the regulatory requirements have been met. This not only prevents common mistakes, but it also frees up valuable time for your compliance team to focus on bigger issues.

Get Buy-in from the Compliance Team

Even an entry-level position as a compliance officer requires an expert level of skill. Many compliance professionals are lawyers, and even those who aren't tend to have advanced degrees and years of industry experience. As the primary users of any compliance technology, it's essential that these subject matter experts are involved in the development and implementation process. They already know where the inefficiencies are, and where improvements will have the most impact.

Automate Reporting Wherever Possible

Compliance reporting can be an unbelievably tedious task, requiring hours of database work, number crunching, and spreadsheet manipulation. Not surprisingly, one of the first technologies to be adopted by compliance professionals was reporting automation. Automated compliance reporting allows for fast-turnaround information gathering and presentation, resulting in documents that even non-experts can easily understand. They also help to remove human error from the process, making these reports more reliable.

Invest in Expertise

Every industry has a specific set of regulatory requirements to adhere to, and every company has a unique combination of use cases, internal policies, and business technologies. There is no one-size-fits-all solution for combining technology and compliance in a meaningful way. Get the solution right, and the efficiency and ROI benefits are huge. Get it wrong, and your compliance "solution" can actually make things worse. It's absolutely essential that your technology implementation partner work closely with every stakeholder to find the right workflows, software, integrations, and training to make your investment in compliance technology worthy of your investment.

UNDERSTANDING CYBERSECURITY - EXTENT OF RISK

WE EAT SOFTWARE

fayedigital.com

WHILE WORKING TO BETTER THE COMPLIANCE WITH YOUR TECHNOLOGY MAY SEEM LIKE A FRUITLESS TASK, IT'S IMPERATIVE.

Cyber criminals are lurking around every corner of the web for medical data, no longer only targeting large healthcare companies. These criminals don't care if you had to quickly switch to a distributed workforce or don't have the funds to heavily invest in IT security. As telemedicine and other web-based medical technologies become more commonplace, however, even smaller healthcare-related providers are increasingly discovering just how vulnerable their systems are to cyberattacks.

One of the biggest concerns for cybersecurity professionals is the security of the patient's own home internet network. Internet-connected health monitoring devices can be powerful tools for remote care. Yet, many of these devices were never designed with data security as priority. Often these devices aren't encrypted, and instead rely on the security of the network they are connected to. This can be a problem if that network is a simple home WIFI setup protected by a common, easily guessed password like "123456" or "password." (Shockingly, both of these passwords are among the most commonly used in home devices according to a 2020 analysis by NordPass.)

If a hacker can access a patient's home network, accessing that patient's medical records through their telemedicine connections is easy. The near-complete lack of FDA regulation on telehealth technology also makes this situation worse. Many doctors offer video consultations using free video conferencing tools like Zoom, FaceTime, or Skype, for instance, without needing to meet any additional privacy requirements. It's not difficult to imagine the damage a hacker could do simply by listening in on these conversations.

CONCLUSION

Creating a truly optimized and positive patient experience is complex. You want to make sure you don't forget one of the most important steps to the patient experience: making sure their personal information is secure.

A HIPAA compliant CRM software platform needs to be managed by a partner that is also subject to HIPAA compliance for Business Associates. HIPAA-compliant technology partners give you the leverage to keep data secure, while bettering the overall patient experience.

Don't let your vendors, business partners, and other third-party associates be the weakest link in your HIPAA compliance chain. Anyone with access to your patients' protected data needs to meet the same standards as your organization. This means regular auditing and training, as well as ironclad contracts spelling out the exact security standards they need to meet before handling any HIPAA-related patient data.

Partnering with third-party vendors who focus on HIPAA compliance can go a long way to ensuring that you continue to be compliant.

Faye offers Healthcare CRM and Financial Services CRM users the technical and physical safeguards that are intended to prevent the unauthorized disclosure or use of their Protected Health Data.

FAYE

At Faye, we love software. We eat it, breathe it, and build it. Our mission is to make the best software in the world even better by helping clients lead the way with software strategy, deployments, integrations and technical support.

With us is better than without us. As an Inc. 5000 award winner eight years in a row, we help mid-market and enterprise clients globally achieve up to 10x productivity returns by leveraging the hidden potential within Zendesk, SugarCRM, Salesforce, HubSpot, and more.

There is no ceiling to what we can achieve with a lot of caffeine and an uncompromising commitment to make software better. We are intensely passionate about eating your software complexity and challenges, so that you don't have to.

Our flagship offering, AXIA by Faye™ bundles our IP, capabilities and pre-built software enhancements into one monthly or annual subscription. The result - A partnership that drives lasting value and optimization even as you grow.

818-280-4820
fayedigital.com

WE EAT SOFTWARE