BRAIDED

October 2024

Safeguard Your PHI with HIPAA Compliance

A Case Study in Compliance Success

Braided Achieves HIPAA Success for Crotched Mountain Foundation

Crotched Mountain Foundation (CMF) is a nonprofit organization dedicated to empowering vulnerable individuals with disabilities and chronic illnesses. Taking care of a broad collection of individuals requires a full spectrum of services, and CMF brings its passion and support to many aspects of its client base, including:

- Case management services
- Affordable independent living through HUD property management
- Specialized day programs
- Accessible outdoor recreation
- Community-based special education and services grant funding

The social service and healthcare nature of CMF's services qualifies its clients as patients, so HIPAA compliance is a must. HIPAA, a federally mandated framework designed to protect patient health information (PHI), comprises two main components: data privacy and security. HIPAA is legally binding and enforceable across all US-based entities regardless of their not-for-profit status.

In recent years, CMF restructured its client offerings while transitioning from a centralized location to a hybrid deployment model. Consequently, CMF would require a comprehensive overhaul of its operational and cybersecurity measures. Operationally, their HIPAA implementation needed to be restructured to fit their updated model. From a security perspective, CMF recognized that implementing additional technology safeguards would enhance cybersecurity while also easing the burden of HIPAA compliance.

Jon Dash, CMF's compliance officer, is experienced in heavy compliance efforts and understands the substantial workload involved in implementing HIPAA:

- Drafting, reviewing, and approving policies and procedures.
- Reviewing and updating ancillary documents
- Assessing cybersecurity policies and tools.
- Performing a gap analysis to identify immediate tasks.
- Implementing high-priority tasks.
- Working with external information technology consultants to implement security measures.
- Gathering, organizing, and documenting evidence to back up compliance claims.

Dash intended to shoulder this workload alongside his regular responsibilities, but a timely referral from within the nonprofit space brought Braided Technologies (Braided) to the table. In late 2023, CMF engaged Braided to shepherd its HIPAA compliance and cybersecurity technology initiatives.

Why Comply?

Legal Protection:

Avoid the legal consequences and contractual defaults that result from non-compliance.

Financial Safeguards:

Compliance irregularities can result in fines and penalties ranging into seven figures—if not more.

Competitive Advantage:

Meet the stipulations of RFPs that require organizations to meet specific data protection standards.

Operational and Security Benefits:

Eliminate operational silos and inconsistencies within your business while improving your data security.

Marketing Edge:

Be seen as a responsible and trustworthy citizen of the world. Enhance your reputation and build consumer trust.

Avoid Bad Press:

Dodge the negative publicity associated with data breaches and non-compliance.

Braided’s Compliance Services

Braided knows that compliance is a multi-faceted challenge consisting of controls, policies, and cybersecurity. Compliance should become habitual instead of a stop-gap effort. At the end of the day, Braided views compliance as essential for aligning operations across the breadth of your company: Dodge operational silos that are inefficient and susceptible to security vulnerabilities!

Aware of the compliance’s broad scope, Braided collaborates with upper management to signal—from the top down—that compliance is a core corporate objective. We operate at both a strategic and tactical level across all teams and departments, weaving a compliance-first approach that integrates seamlessly with your operations. Braided tailors its methods to minimize client workload. As we work to adjust your operations, we prioritize making a smooth and comfortable compliance journey.

Making Compliance Happen

Braided balances its compliance expertise with a technology focus with a two-phased approach to achieving and maintaining compliance.

Phase 1: Scoping and Goals

1. Implement a GRC (governance, risk, and compliance) tool to assist with your specific compliance efforts.
2. Craft and customize policies and procedures that encompass current and near-future compliance frameworks.
3. Perform a gap analysis to identify immediate tasks and map out a proactive timeline to achieve continuous compliance objectives.
4. Address urgent compliance issues (e.g., external assessment requests).

Phase 2: Low Stress and Continuous Compliance

1. Weave compliance and technology into the corporate technology and budget timelines.
2. Involve stakeholders across the organization to review and update ancillary documents like the employee handbook.
3. Assess existing cybersecurity policies and tools, remediating gaps as required.
4. Gather, organize, and document evidence to back up compliance claims.
5. Refine policies and procedures, as necessary.
6. Tackle additional compliance frameworks while leveraging current efforts.

Compliance Cadence

Meeting the requirements set by any framework or regulation might appear daunting but breaking it down into smaller parts makes it more manageable.

Braided recommends a consistent, “small bites” approach to systematically chip away at compliance tasks. Additionally, we encourage clients to treat compliance documents as living documents.

Fractional Compliance Positions

Having full-time employees for compliance roles such as data privacy officers, compliance officers, and internal auditors can be cost-prohibitive. Braided offers both expertise and personnel to fulfill these essential compliance functions within your organization. By partnering with Braided, you can access these critical resources as needed without the burden of full-time overhead.

Billing

To minimize cash flow impacts on our clients, Braided bills for our consulting expertise plus the compliance tool on a monthly, recurring basis. This approach aligns with our compliance philosophy, emphasizing consistent, manageable efforts. Braided keeps its billing straightforward and user-friendly.

CMF Reclaims HIPAA Compliance

CMF’s senior management agreed that Braided’s measured cadence would ease the transition into HIPAA compliance. Implementing Braided’s compliance-as-a-habit (CaaH) approach successfully guided CMF’s corporate practices into HIPAA adherence, achieving key milestones in just a matter of months. Additionally, CMF leveraged a newly acquired GRC tool to support the gathering of evidence, as well as the generation of reports, assessments, and presentations for both internal and external stakeholders.

Policy adoption was quick, enabling stakeholders to set the CMF’s compliance goal line. This speedy adoption positively impacted all subsequent compliance efforts, resulting in a stress-free and expedited rollout.

Adopt the policies, set the goals, and get to work!

Aside from operational concerns, HIPAA requires that all employees be versed in data privacy and security. CMF leveraged a third-party learning management system (LMS) to track employee training on HIPAA regulations and data security. CMF’s GRC tool aggregated and stored training data and policy attestation reports as evidence of compliance.

CMF also focused on vendor management. Vendor relationships were safeguarded by either a business associate agreement (BAA) or confidentiality agreement, depending on each vendor’s interaction with PHI. CMF’s GRC tool tracked the vendor list, relationship types, contracts, and required documents.

Each aspect of compliance was placed on a review schedule to ensure continued adherence. Braided’s Compliance-as-a-Habit approach prioritizes measured compliance refinement and integration into a client’s standard business operations.

Which Compliance Tool Is Right for You?

To make the magic happen, Braided outfits your company with a governance, risk, and compliance (GRC) platform that fits your company's needs. Depending on the complexity of your technology stack and corporate objectives, we can automate evidence collection as needed in your compliance journey. Additionally, our vetted GRC tools manage a company's policy documentation.

GRC tool features may include:

Evidence Collection via Tech Stack Integrations	Natively connect to your tech stack to collect up-to-date evidence.
Unified Framework Controls	Break down multiple complex compliance frameworks into a common set of controls, allowing extreme clarity around how these frameworks overlap.
Policy Management	Leverage a comprehensive library of auditor-approved policies. Clients can customize, deploy, and document directly within the platform.
Process Control	Highlight priority tasks on an audit dashboard to focus compliance efforts.

Braided will work with you to choose a tool that will best boost future compliance efforts with the minimum of repetitive work.

Braided's Approach: Compliance-as-a-Habit

At Braided, we are transparent in our approach to compliance. Compliance should become a reflex—a set of simple habits that you consistently implement. We view your policies and procedures as living documents that should be regularly reviewed and updated. Developing these habits pays off by ensuring that future compliance assessments are smooth and do not disrupt your business operations.

Our process begins by establishing policy and procedure documents. Creation of these documents serves as an opportunity to eliminate information silos, making your business more efficient and resilient in the face of change. These documents are the foundation of all compliance work.

Once your goals are identified and codified, we work with you to:

- ✓ Onboard the integration of the GRC tool with your tech stacks to monitor compliance.
- ✓ Identify and interface with key stakeholders (e.g., HR, technology, and operations).
- ✓ Review cyber and general insurance coverages.
- ✓ Assign responsibilities throughout the organization.
- ✓ Work with stakeholders to update procedures.
- ✓ Gather compliance evidence.
- ✓ Perform a full gap analysis to identify remediation tasks.

With compliance in place, we then schedule regular reviews of your documents while evaluating them against current business needs to identify improvement opportunities.

This is just the start of how Braided can simplify compliance with minimal interruption to your daily work. We keep meetings short and to the point, respectful of your time.

Once in place, Braided's approach and fractional compliance officers work continuously in the background, requiring no dedicated teams or extensive time commitments from you.

We believe setting reasonable, easily- achieved compliance deadlines is the path to continual improvement within an organization's fabric. We recommend letting Braided guide you through the process, making compliance into a painless effort.

Slow and steady wins the race!

> **Partnering with Braided was truly a strategic win for our organization. With their guidance, our cybersecurity and HIPAA compliance initiatives were completed in record time.**
>
> *— Jon Dash,*
> *Crotched Mountain Foundation*

Delivering a Competitive Advantage Through Habitual Compliance and Technology Innovation.

Visit braided.tech or set up a free consult to see how Braided's compliance services can fit your exact needs.