BARR ADVISORY

2026 Whitepaper

The Healthcare Compliance Journey

How BARR Supports You At Every Stage

TABLE OF CONTENTS

Introduction

Organizations that create, store, transmit, or process protected health information (PHI) face a growing set of regulatory expectations and security risks. As digital healthcare ecosystems expand, safeguarding sensitive data is no longer just a technical responsibility—it is a business imperative.

At the same time, the number of available frameworks and regulatory requirements continues to expand. From HIPAA and HITRUST to SOC 2, ISO 27001, and government-focused programs such as FedRAMP and CMMC, organizations are often faced with difficult decisions about where to begin and how to prioritize their efforts. Selecting the right path requires a clear understanding of organizational goals, industry expectations, and risk tolerance.

This guide is designed to help healthcare organizations navigate the evolving compliance landscape with clarity and confidence. It explores the foundations of regulatory compliance, outlines key frameworks that support security and risk management, and highlights strategies for building a scalable program that grows alongside your business. By taking a thoughtful, structured approach, organizations can transform compliance from a regulatory burden into a strategic advantage that strengthens trust and supports long-term success.

As digital healthcare ecosystems expand, safeguarding sensitive data is no longer just a technical responsibility—**it is a business imperative.**

HIPAA Compliance: Building the Foundation

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was first signed into law in the U.S. in 1996 to establish policies and procedures for maintaining the security and privacy of individually identifiable health information, also known as protected health information or PHI. The law not only defines standards, but also outlines offenses and creates civil and criminal penalties for violations.

HIPAA has gone through many iterations over the years. In the early 2000s, the **HIPAA Privacy Rule** was added to ensure individuals' health information is properly protected while allowing the flow of health information needed to provide high-quality healthcare and protect the public's health and well-being.

In 2005, the U.S. Department of Health and Human Services (HHS) created the HIPAA Security Rule, which added regulations for protecting patients' electronic PHI (ePHI) and preventing it from being disclosed without the patient's consent.

Another update was issued in 2009, when the HITECH Act introduced breach notification requirements and increased civil penalties for HIPAA violations based on the nature and extent of the breach, as well as harm caused by the incident.

Who Must Comply with HIPAA?

HIPAA is not a voluntary framework or best practice—it is a federal law that applies to specific types of organizations and carries significant legal and financial consequences for noncompliance. Organizations that process, store, and interact with PHI and ePHI must comply with HIPAA. This includes "covered entities" such as:

- **Healthcare providers** and other health services organizations that transmit PHI to perform transactions like claims, determine benefit eligibility, and field referral authorization requests.
- **Health plans**, such as insurance providers and other organizations that help individuals and groups pay for healthcare services.

- **Healthcare clearinghouses**, or organizations that process other entities' healthcare transactions for tasks like claims processing, billings, and data management.

HIPAA also applies to individuals and organizations outside of these covered entities ("**business associates**") who use or disclose individually identifiable health data to perform or provide services.

Unlike frameworks such as SOC 2, which organizations may choose to adopt, HIPAA compliance is mandatory for organizations that meet these definitions. Failure to comply can result in substantial penalties enforced by the HHS Office for Civil Rights (OCR), including civil fines ranging from hundreds to millions of dollars, mandatory corrective action plans and ongoing audits, and potential legal liability.

Some organizations may also choose to maintain compliance with HIPAA even if not required by law in order to align with best practices and build trust with customers and stakeholders.

What is Required for Security Compliance?

According to HHS, the goal of the HIPAA Security Rule is to protect ePHI through administrative, physical, and technical safeguards:

- **Administrative:** This includes controls related to risk analysis and risk management, termination procedures, access authorization, password management, data backup plans, and disaster recovery plans.
- **Physical:** This includes controls related to facility access, workstation use and security, and device and media controls such as data backup and storage.
- **Technical:** This includes controls related to unique user identification, emergency access procedures, encryption, and decryption.

While not all of these controls are required for every organization, they are each designed to ensure the confidentiality, integrity, and availability of all ePHI that an organization interacts with as well as protect against reasonably anticipated threats and unauthorized disclosures of ePHI.

What is Required for Privacy Compliance?

The HIPAA Privacy Rule encompasses several key elements designed to protect patient information. This includes the "Minimum Necessary" standard, which requires PHI to be disclosed only to the extent necessary to accomplish the intended purpose. Additionally, the rule mandates covered entities provide patients with a Notice of Privacy Practices, informing them of their rights and how their information will be used and disclosed.

Another critical element is the requirement for covered entities to obtain patient authorization before using or disclosing PHI for purposes not otherwise permitted by the rule. Patients also have the right to access their medical records, request corrections, and receive an accounting of disclosures of their PHI.

For patients, the HIPAA Privacy Rule provides significant protections for their personal health information. It ensures that their medical records and other PHI are safeguarded against unauthorized access and misuse. Patients have the right to receive a copy of their health records and request that corrections be made to any inaccuracies.

The rule also empowers patients by giving them control over how their information is used and disclosed. They can specify restrictions on certain uses and disclosures and have the right to be informed about privacy practices and their rights under the rule. This transparency and control help build trust between patients and healthcare providers.

Organizations subject to the HIPAA Privacy Rule must adopt comprehensive compliance strategies to ensure adherence to regulations. This includes conducting regular risk assessments to identify potential vulnerabilities and implementing corrective actions to address any gaps. Training staff on HIPAA compliance and the importance of protecting PHI is also crucial.

Additionally, organizations should develop and enforce policies and procedures that align with HIPAA standards. This includes establishing protocols for responding to data breaches and ensuring that business associate agreements are in place to safeguard PHI when shared with third-party service providers. Regular audits and monitoring can help your organization avoid HIPAA violations, maintain compliance, and mitigate risks associated with handling PHI.

How Can Organizations Validate HIPAA Compliance?

Unlike compliance frameworks such as HITRUST CSF and ISO/IEC 27001, there is no formal certification available or required to prove HIPAA compliance.

However, there are other options for organizations that want to provide assurance to customers that they adhere to the strict security standards outlined by HIPAA. One way is to obtain a **report on HIPAA compliance** provided by a third-party auditing firm, like BARR Advisory. BARR's attest services team can assess your cybersecurity program against HIPAA requirements and provide a formal report on their conclusions.

Organizations can also pursue compliance with other frameworks that weave elements of HIPAA into their requirements. This includes HITRUST, an internationally accepted standard for security compliance that was designed with HIPAA in mind.

Another option is SOC 2. Many common trust services criteria (TSC) used in SOC 2 reporting align with HIPAA Security Rule requirements. For organizations also interested in pursuing a SOC 2 report, BARR's attest services team can assess whether controls related to access management, risk management, and asset management are designed to meet HIPAA regulations.

Navigating the Journey to HIPAA Compliance

Before you embark on a journey to assess your organization's HIPAA compliance, BARR's consulting team can perform a **HIPAA readiness assessment** to help identify existing gaps in your security program and provide recommendations for remediation. They can assist with tasks such as:

1. Understanding Your Scope

Start by determining whether your organization handles PHI and how that data flows through your environment. This includes identifying where data is stored, how it's transmitted, and whether it's shared with third parties. Understanding your role as a covered entity or business associate is critical to defining your compliance obligations.

2. Conducting Risk Assessments

Conducting regular risk assessments is a required element of HIPAA compliance. Organizations must take steps to identify potential vulnerabilities, evaluate risks, and document their findings. It's also important to outline policies that define how identified risks are addressed and mitigated.

3. Implementing Strong Policies and Procedures

Effective HIPAA compliance requires more than intent—it requires documentation. Organizations should clearly define who has access to PHI and why, what security measures are in place, and how incidents are detected and handled.

4. Training Your Team

Even the most robust security program can fail without employee awareness. HIPAA training is mandatory and should be ongoing, ensuring staff understand their responsibilities and company procedures. Training should also be documented to demonstrate compliance and accountability.

5. Strengthening Access Controls

Limiting access to PHI is essential. Organizations must establish clear authorization protocols and authentication requirements to ensure only the right individuals can access sensitive data. It's also important to outline how misuse or unauthorized access will be detected and addressed.

6. Managing Vendor Risk

Third-party vendors are a common source of HIPAA violations. A strong vendor management program should include thorough risk assessments, clear documentation of data access and usage, and contractual safeguards to prevent unauthorized disclosures. Understanding how vendors interact with your data helps reduce the likelihood and impact of a breach.

7. Preparing for Breaches Before They Happen

No organization is immune to a data breach. That's why having a documented and tested incident response plan is critical. Your plan should define steps to contain and remediate the breach as well as the roles of each team member in executing the plan. Testing these processes regularly ensures your organization can respond quickly and effectively when an incident occurs.

Third-Party Auditing: Taking the Next Step

While internal policies and procedures form the backbone of a strong compliance program, many organizations seek independent validation to demonstrate the effectiveness of their security controls. Third-party auditing provides objective assurance that safeguards are properly designed and operating as intended.

Frameworks such as SOC 2 and HITRUST allow organizations to formally evaluate their environments against recognized standards. These assessments not only strengthen internal security practices but also provide customers, partners, and stakeholders with confidence that sensitive data is being handled responsibly.

SOC 2

A SOC 2 examination reports on one or any combination of the AICPA's trust services criteria —security, availability, processing integrity, confidentiality, and privacy. It demonstrates an organization's commitment to its consumer requirements and cybersecurity best practices.

SOC 2 reports meet the needs of a broad range of users who require detailed information and assurance about the controls at a service organization. The report can play an important role in oversight of the organization, vendor management programs, and internal corporate governance and risk management processes.

The duration for your SOC 2 report depends on the type you acquire. If your organization has previously documented your controls through an automation partner, Type 1 reports may be performed right away. Type 1 reports offer a point-in-time service, testing your design on a specific date. Type 2 reports are generally audited throughout a three to 12-month period. SOC 2 reports reflect your organization's operating effectiveness during the course of a review period and provide a more detailed assessment of your controls.

A SOC 2 report is typically relevant for service organizations that provide services involving the processing of sensitive customer information or data. This framework is particularly valuable for businesses that offer technology and cloud computing services, data hosting, managed IT services, Software as a Service (SaaS), and various other outsourcing services. While not industry-specific like some other compliance frameworks, SOC 2 is widely recognized and utilized across different sectors, including healthcare.

HITRUST

The HITRUST CSF is a comprehensive, threat-adaptive standard designed to help organizations strengthen their security posture and build trust with customers, partners, and stakeholders.

Recognized internationally, HITRUST stands out for its flexibility and responsiveness to emerging threats. Because the framework is updated more frequently than standards like SOC 2 or ISO 27001, it is better equipped to help organizations across industries keep pace with today's fast-evolving risk landscape.

Organizations pursuing HITRUST certification can choose one of three assessment options that provide varying levels of assurance:

- The **e1 certification** covers 44 foundational security controls and is ideal for low-risk organizations and early-stage startups to demonstrate adherence with baseline security best practices.
- The **i1 certification** adds 138 controls, for a total of 182, and provides a moderate level of assurance for businesses with more robust information security programs and greater assurance needs.
- The **r2 certification** is designed for organizations with complex environments that need the highest levels of assurance. The most rigorous of the three options, the r2 requires 200 or more controls, depending on the scope of the assessment.

For organizations looking for validation of essential cybersecurity controls, pursuing e1 certification is a smart option that paves the way for more robust assessments in the future. BARR experts recommend the e1 assessment to startups or other organizations that are just getting started in their cybersecurity journey. The certification is valid for one year from its issuance date; after that year, BARR experts recommend building on the established cybersecurity foundation with a higher-level assessment, like the i1 or r2.

The HITRUST i1 assessment is a good choice for any vendor looking to provide a moderate level of assurance on transparency, accuracy, consistency, and integrity. It allows smaller organizations with less support staff to become HITRUST certified. This is because the i1 only addresses the implementation of each control as opposed to the r2 which requires a policy, procedure, and the actual implementation of the control.

The r2 certification is valid for two years with an interim period in between. It addresses five key areas—policy, procedures, implementation, measurement, and management—and over 200 controls. The r2 is the right assessment for established organizations who obtain a significant volume of sensitive data and PHI to keep secure. As the most comprehensive of the HITRUST assessments, the r2 is key for organizations that need high-level assurance and have the necessary resources and team dedicated to complete a larger, more complex assessment.

Which Framework is Right For You?

Both HITRUST assessments and SOC 2 examinations focus on information security controls. HITRUST is specifically designed for the healthcare industry and incorporates industry-specific requirements, while SOC 2 is more general and applicable across various sectors with a focus on trust service criteria.

Organizations often choose the framework that aligns with their industry, regulatory requirements, and specific business needs.

For some organizations, like ThreeFlow, achieving compliance against both frameworks can be a powerful differentiator.

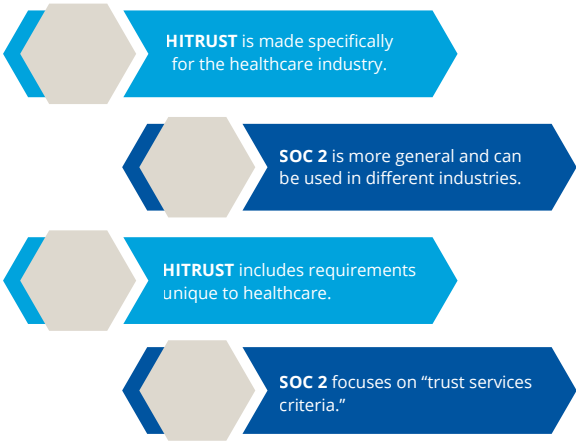
ThreeFlow is the world's first Benefits Placement System—a new category of enterprise software that streamlines benefits placement by connecting brokers, carriers, and employer clients in a single, shared system. Serving a highly regulated industry, ThreeFlow prioritizes robust security measures to align with the stringent requirements of its partners, customers, and their end clients.

Since 2021, ThreeFlow has partnered with BARR Advisory to navigate its compliance journey, achieving multiple attestations, including SOC 2 Type 2 and HITRUST e1, with the goal of reinforcing trust and cementing its place as a true market leader.

"From Day 1, security, compliance, and governance has been a first-class citizen in our architecture decisions, in our product development decisions, and how we imagine this company growing," said Shaheeb Roshan, co-founder and CTO of ThreeFlow.

With a strong security foundation already in place, the ThreeFlow team sought BARR's guidance in refining its compliance roadmap and ensuring its security infrastructure was prepared for future growth.

"When we first engaged with BARR, we did so from a position of fairly good readiness…and a clear picture of where we needed to go," Roshan said. "But we couldn't take those next steps without the support and guidance from BARR Advisory."



Rather than taking a reactive approach to compliance, ThreeFlow worked with BARR to align its security efforts with its business trajectory. This forward-thinking strategy was particularly valuable as the company expanded into new market segments, including medical benefits, which requires adherence to even more rigorous security standards.

With SOC 2 Type 2 and HITRUST e1 certifications in place, ThreeFlow has significantly reduced the time spent on security questionnaires required by partners and customers.

"Now, our market directors are trained to dive headfirst into the security and compliance governance question," Roshan said. Supplying a SOC 2 report right off the bat "has materially reduced our administrative time for getting agreements and contracts finalized with our customers and our partners," he said.

As ThreeFlow continues its rapid growth, security and compliance will remain core to its mission. With SOC 2 Type 2 and HITRUST e1 certifications in place, the company is well-positioned to expand its market presence, deepen trust with partners, and set the benchmark for security excellence in its industry.

Grow Your Compliance Program: Scaling with Advanced Compliance Frameworks

While SOC 2 and HITRUST can help provide a foundation for establishing strong security and compliance practices, many organizations transition to more robust compliance frameworks as the company and its security program grow. Here are some options to consider.

ISO 27001 and Related Frameworks

ISO/IEC 27001:2022—often simply called **ISO 27001**—is an international standard that helps organizations establish, implement, and maintain an information security management system (ISMS). Obtaining certification to ISO 27001 is a valuable way to differentiate your organization as it demonstrates your compliance with industry standards and helps your organization manage the security of your services, data, intellectual property, or any information entrusted to you by a third party.

For organizations operating in international markets, ISO 27001 is often expected by customers. Notably, there are many similarities between ISO 27001 and HITRUST. Both prioritize data protection through rigorous security controls that support regulatory compliance. Each promotes a structured approach to risk management and governance, helping organizations secure sensitive information and meet industry standards, while maintaining scalability and flexibility to meet your organization's needs as you grow.

"ISO 27001 is part of the foundation that the HITRUST framework was built upon, which is why HITRUST CSF can help satisfy the requirements of ISO 27001," said Steve Ryan, who leads BARR Advisory's healthcare services.

While the two standards can help you meet requirements on an individual basis, your organization might choose to pursue both certifications for a number of reasons, including:

- Ensuring a high level of trust with both national and international customers
- Increasing security over your ISMS and PHI
- Achieving compliance requirements with greater reliability
- Differentiating yourself in the marketplace

Organizations seeking ISO 27001 certification may also choose to pursue other certifications that align well with the standard. For instance, **ISO 27701**, which focuses on data privacy, was specifically designed for organizations that process personally identifiable information (PII). ISO 27701 outlines requirements for establishing, implementing, maintaining, and continually improving a privacy information management system (PIMS).

ISO 27017 is an internationally accepted compliance standard that serves as an extension of ISO 27001 with a specific focus on cloud security. Achieving ISO 27017 certification requires seven additional controls that are unique to cloud services, as well as 37 controls that are implemented through ISO 27002. The framework covers a wide range of areas, including data protection, access control, incident response, and risk management.

ISO 27018 is another extension of ISO 27001 that provides a privacy-specific framework for cloud service providers (CSPs) that process PII. It adds 24 additional controls that are unique to CSPs. Those controls are focused on safeguarding PII in cloud environments, such as secure data deletion, restrictions on processing, and user transparency.

ISO 27017 and ISO 27018 are not a standalone certifications; they must be achieved alongside an ISO 27001 certification.

For organizations that use, produce, or develop artificial intelligence tools, ISO 42001 is also a smart framework to consider. It mandates numerous controls for establishing, operating, monitoring, and continually improving an organization's AI management system (AIMS). To achieve ISO 42001 certification, an organization must have deep-rooted methodologies for ensuring the ethical, responsible use of AI, along with an established framework to help identify, manage, and reduce risks related to AI use and development. Achieving ISO 42001 certification shows that an organization has taken steps to ensure its use and development of AI is ethical, transparent, and aligned with global best practices.

FedRAMP

Established in 2011, the Federal Risk and Authorization Management Program (FedRAMP) is a U.S.-based cloud security framework aimed at ensuring sensitive federal government data remains protected. The government-wide program standardizes security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies. It's built on the security controls defined in NIST 800-53, which sets specific requirements for areas such as access control, vulnerability management, system monitoring, and incident response.

Achieving FedRAMP authorization not only demonstrates that your solution meets rigorous security requirements but also opens doors to the federal marketplace. However, it is a meticulous process that requires careful planning and the assistance of a qualified Third-Party Assessment Organization (3PAO). To complete the authorization process, CSPs must partner with a federal agency that is willing to sponsor them.

At BARR Advisory, our team of experienced FedRAMP experts can help put you on the path to success. From readiness assessment to continuous monitoring, we provide comprehensive support and guidance at every stage of your FedRAMP journey. Partnering with BARR ensures you're equipped to achieve and maintain compliance with confidence.

CMMC

For organizations that want to do business with the U.S. Department of War (DoW), the Cybersecurity Maturity Model Certification **(CMMC)** is a key framework to familiarize yourself with. CMMC was developed to ensure all DoW contractors follow cybersecurity best practices based on the level of risk their work involves.

CMMC was specifically designed to protect two types of sensitive information:

- *Federal Contract Information (FCI):* This includes communications related to government contracts, such as contract details, RFPs, and other collaborative documents.
- *Controlled Unclassified Information (CUI):* This includes sensitive but unclassified government information, such as technical schematics, research data, and procedural documents. While not technically classified as "secret" or "top-secret," CUI still presents a national security risk if exposed.

Even if you don't yet have a government contract, beginning the CMMC readiness process now—including conducting a gap assessment and understanding how your environment aligns with the DoW's requirements—can help you secure future opportunities. With deep expertise in cybersecurity and government contracting, BARR Advisory simplifies the CMMC process with end-to-end consulting, including gap analysis, implementation support, and ongoing compliance maintenance. Our expert CMMC consultants guide you every step of the way, helping you meet DoW standards and grow your government contracting opportunities.

FDA Compliance

For organizations operating in the healthcare technology and medical device sectors, compliance with U.S. Food and Drug Administration (FDA) regulations is an essential component of managing risk and protecting patient safety. The FDA establishes requirements for the development, testing, and maintenance of medical devices, including software-based and connected technologies that process sensitive patient data.

FDA compliance often involves implementing quality management systems, maintaining thorough documentation, conducting risk analyses, and validating that systems perform safely and effectively throughout their lifecycle. Organizations must also establish processes for monitoring device performance, reporting adverse events, and managing updates or changes to regulated technologies.

As healthcare solutions increasingly rely on software and connected devices, aligning cybersecurity and regulatory requirements becomes even more critical. Establishing strong controls early can help streamline FDA submissions, reduce delays, and support long-term product reliability.

A Compliance Journey Mapped to Your Strategic Goals

Building a successful compliance program requires more than understanding individual frameworks—it requires a clear roadmap that aligns security efforts with long-term business goals. With so many standards, regulatory requirements, and risk considerations to evaluate, organizations often struggle to determine which initiatives should come first and how to sequence them effectively.

To help organizations navigate this complexity, BARR Advisory has developed the **Compliance Compass**, a free online tool designed to guide governance, risk, and compliance (GRC) teams through every stage of the compliance journey. The tool helps organizations identify goals that align with their growth strategy and build a customized roadmap that prioritizes key security initiatives.

Developed in collaboration with cybersecurity and compliance experts, the Compliance Compass delivers tailored recommendations based on an organization's industry, size, and stage of maturity. It provides actionable insights that help teams understand the requirements of leading frameworks and plan the steps necessary to achieve alignment. From early readiness activities to advanced certification planning, the tool supports organizations as they build a focused and scalable compliance strategy.

Take the two-minute assessment now to get started.

> ***"ISO 27001 is part of the foundation that the HITRUST framework was built upon, which is why HITRUST CSF can help satisfy the requirements of ISO 27001."***
>
> Steve Ryan,
> Service Line Leader,
> Attest Healthcare

Conclusion

Navigating the evolving compliance landscape can feel overwhelming, but organizations that take a structured, proactive approach are better positioned to manage risk, strengthen trust with patients, and support long-term growth. By leveraging tools like **BARR's Compliance Compass** to clarify priorities and map next steps, organizations can move beyond uncertainty and build a compliance strategy that aligns with their business objectives. With the right roadmap in place, compliance becomes more than a requirement—it becomes a foundation for trust, accountability, and success.

About BARR Advisory

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. Serving some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

Our Services & Frameworks

SOC Examinations
[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]

ISO Certification
[27001, 27017, 27018, 27701, 42001, 9001, 22301]

Healthcare Compliance
[HIPAA/HITRUST]

Government Compliance
[FedRAMP, GovRAMP, CMMC, DFARS, NIST]

Privacy & Data Protection
[GDPR, CCPA, GLBA, PCI DSS, CSA STAR, Microsoft DPR]

Advisory & Managed Services

GRC & Engineering

Assessments

Attestation & Certification

CONNECT WITH BARR

Want to learn more about our healthcare security and compliance services? Contact us today.