feroot

WINTER 2026 High Performer | WINTER 2026 Best Support | BEST SOFTWARE 2026 Top 50 DATA PRIVACY PRODUCTS | WINTER 2026 Easiest To Do Business With | FALL 2025 High Performer

# The Hidden Compliance Crisis in Healthcare

## Why 2026 Demands a Shift to Continuous, AI-Driven Compliance

# Contents


Introduction: The Illusion of Compliance . . . . . 3

The Hidden Risk in Modern Digital Experiences . . . . . 4

How Compliance Breaks in Practice . . . . . 5

Why Enforcement Is Accelerating . . . . . 6

The Real Problem: Time, Evidence, and Proof . . . . . 7

What's Changing in 2026 . . . . . 8

What to Do Now: Your 2026 Compliance Checklist . . . . . 9

A New Approach to Compliance: Feroot . . . . . 10

Glossary: Key HIPAA Digital Experience Definitions . . . . . 13

INTRODUCTION:

# The Illusion of Compliance

Most healthcare organizations believe they are compliant. Consent banners are live, CMPs are configured, risk assessments are completed, and policies are documented across teams.

On paper, everything appears to be in order.

And yet, organizations with mature compliance programs are still facing lawsuits, enforcement actions, and multi-million-dollar penalties. Not because they ignored compliance, but because the definition of compliance has changed.

What used to be a static, point-in-time exercise is now something far more demanding.

Compliance is no longer something you configure. It is something you must continuously validate and prove.



Book a Demo

# The Hidden Risk in Modern Digital Experiences

Healthcare's digital footprint has expanded rapidly. Patient portals, mobile apps, telehealth platforms, and online scheduling systems are now central to care delivery, and fully in scope from a compliance perspective.

## 96% of healthcare websites run online tracking technologies

At the same time, these experiences are deeply instrumented. Research shows that more than 96% of healthcare websites run online tracking technologies, including analytics tools, pixels, chat widgets, and embedded SDKs.

These technologies operate inside the user experience itself. They can capture search queries, form inputs, appointment details, and behavioral data which often qualify as Protected Health Information (PHI).

The challenge is not just data collection, but where that data goes. Most third-party vendors receiving this information are not covered by Business Associate Agreements (BAA), meaning they are not authorized to process PHI.

This risk extends beyond websites. Mobile applications introduce an additional layer of complexity through SDKs, which can silently transmit device identifiers, location data, and in-app behavior to external vendors. These data flows are often harder to detect and control, making mobile apps a significant—and frequently overlooked—source of exposure.

The result is a digital environment where sensitive data is constantly in motion, often in ways organizations do not fully understand.

# How Compliance Breaks in Practice

Most compliance programs are built around configuration. Systems are set up with the expectation that they will behave as intended.

In reality, digital environments are dynamic.

When a user loads a page or opens an app, scripts and SDKs execute immediately. Some are necessary, while others are tied to analytics, marketing, or third-party integrations. These technologies often operate before consent is applied, after it is declined, or inconsistently across different pages and sessions.

This is where compliance breaks—not in policy, but in execution.

Marketing activity is a common trigger. A campaign launches, tracking technologies are added, and the campaign ends. But the underlying scripts remain, continuing to collect data long after their purpose has passed.

Months later, a user interaction is captured, sometimes as simple as a screenshot, and becomes the basis for a legal claim. By then, the original configuration is gone, and the organization is left trying to reconstruct what happened.

## Why Consent Alone Is Not Compliance

Many organizations rely on a Consent Management Platform (CMP) and assume that once it is deployed, compliance is achieved.

In practice, a CMP governs how consent is presented and recorded, not how technologies behave at runtime.

Research and enforcement patterns consistently show that tracking technologies may load before consent is given, continue after it is declined, or behave inconsistently across environments. These gaps are not always visible in configuration, but they are very real in execution.

A Consent Audit closes this gap. It validates whether consent and privacy controls are actually working across every page, workflow, and application screen, not just how they were intended to function.

Without this level of validation, organizations are not verifying compliance but assuming it.

# Why Enforcement Is Accelerating

Organizations are no longer evaluated based on intent or documentation. They are evaluated based on what actually occurred during user interactions.

This shift has introduced a new form of risk: runtime liability.

Enforcement is being driven by multiple factors, including private right of action laws, expanding interpretations of wiretapping regulations, and increased scrutiny around deceptive practices. At the same time, healthcare organizations must navigate a fragmented landscape of overlapping state and federal regulations.

## What This Looks Like in Practice

The impact is already visible. Between 2023 and 2025, healthcare and digital health organizations faced more than $100 million in penalties tied to online tracking technologies.

In 2024, GoodRX settles a lawsuit for $25 million in response to its use of website tracking technologies that leaked visitor data.

Source

In one case, GoodRx was fined for sharing sensitive health-related data with advertising platforms through embedded tracking technologies. In another, BetterHelp faced enforcement for disclosing user data related to mental health to third parties. Large healthcare providers, including Kaiser Permanente, have also been scrutinized for tracking technologies operating on patient-facing pages.

These cases share a common thread: organizations believed they were compliant, but lacked visibility into how data was actually flowing through their digital environments.

## The Three Forces Reshaping Compliance in 2026

This acceleration is not random. It is being driven by three converging forces.

First, enforcement of online tracking technologies has made it clear that websites and mobile apps are fully in scope. Transmitting PHI to third parties without proper authorization or BAAs is now a primary source of enforcement.

Second, the upcoming HIPAA Security Rule changes eliminate “addressable” safeguards. Controls such as encryption, MFA, and real-time monitoring are becoming mandatory across all systems handling ePHI.

Third, HIPRA expands health data regulation beyond traditional HIPAA boundaries, bringing consumer apps, wearables, and digital health platforms into scope.

Together, these forces are making compliance more comprehensive, more prescriptive, and more enforceable.

## The Real Problem: Time, Evidence, and Proof

One of the most overlooked risks in compliance is time.

Organizations often achieve compliance at a specific moment, like after an audit or remediation effort, but that state does not persist. Digital environments change continuously, creating what can be described as fractional compliance.

The challenge is that enforcement actions do not focus on the present. They focus on what happened months earlier.

When asked to demonstrate what occurred during that time, most organizations cannot. Logs are incomplete, configurations have changed, and evidence no longer exists.

This creates a fundamental disadvantage. Without a continuous record of digital behavior, organizations are effectively defending themselves blind.

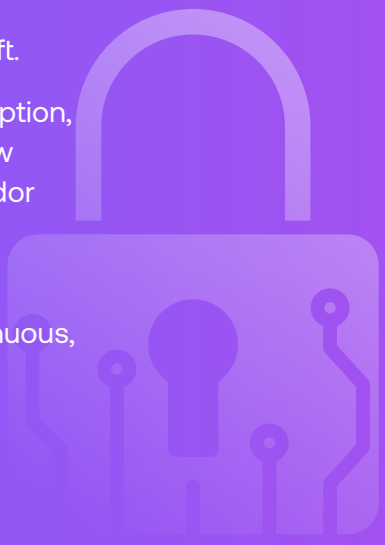
In modern compliance, evidence is not optional. It is the difference between defensibility and liability.

### What’s Changing in 2026

The proposed updates to the HIPAA Security Rule formalize this shift.

Safeguards that were once flexible are becoming mandatory. Encryption, MFA, real-time monitoring, and structured risk management are now baseline expectations. Security testing, system hardening, and vendor accountability are more clearly defined, with stricter timelines and enforcement.

At a high level, the direction is clear: compliance is becoming continuous, standardized, and measurable.



# What to Do Now: Your 2026 Compliance Checklist

Understanding the shift is only the first step. The next is operationalizing it. With enforcement already underway and regulatory timelines tightening, organizations should begin taking action now.

Use the checklist below to assess where your organization stands and where to focus next.

### Expand your compliance perimeter to include websites and mobile apps

Treat all digital experiences as regulated environments. Ensure visibility into every script, pixel, and SDK operating across these properties—not just backend systems.

### Validate runtime behavior—not just configuration

Consent configuration is not the same as compliance. Conduct ongoing validation, such as a Consent Audit, to confirm that tracking technologies behave correctly across every page, workflow, and application screen.

### Inventory and review all third-party technologies

Identify every vendor operating within your digital environments and understand what data they collect, process, and transmit.

### Strengthen vendor governance and BAAs

Ensure all vendors with access to PHI are covered by valid Business Associate Agreements, and verify that subcontractors and OTT vendors meet updated regulatory expectations.

### Implement mandatory technical safeguards

Confirm that encryption, multi-factor authentication, real-time monitoring, and defined backup and recovery processes are fully implemented across all systems handling ePHI.

### Establish continuous monitoring and evidence collection

Move beyond periodic audits. Implement continuous discovery, real-time validation, and persistent logging to maintain a defensible record of compliance over time.

# A New Approach to Compliance: Feroot

The standard for compliance has changed.

Organizations are no longer judged on what they intended to do, or what their policies state. They are judged on what actually happened—and whether they can prove it.

Feroot was built for this new reality.

It provides continuous visibility into digital environments, identifying every script, pixel, and SDK running across websites and mobile apps. It maps how data flows between vendors, detects where PHI may be exposed, and surfaces issues in real time.

At the same time, Feroot performs continuous Consent Audits, validating that privacy controls function correctly across every page and application screen—not just in configuration, but in practice.

This combination of discovery, validation, and evidence allows organizations to move from reactive compliance to continuous, defensible compliance.

## Ready to Shift to Continuous Compliance?

If your organization is still relying on periodic audits and static controls, the gap between what you believe is happening and what is actually happening may already be creating risk.

**Feroot helps close that gap.**

**Get a personalized demo to see how continuous monitoring, Consent Audits, and real-time visibility can transform your compliance posture.**

Book a Demo



Book a Demo

# GLOSSARY

| | |
|---|---|
| **Regulated Entity** | Any healthcare organization or entity that is covered under HIPAA and responsible for protecting patient data. |
| **Vendor / Third Party** | A technology provider engaged by a regulated entity to deliver services such as analytics, marketing, infrastructure, or application functionality. These vendors may have access to data processed within digital experiences. |
| **Authenticated Pages** | Web pages, portals, or application screens that require a user to log in. These environments often collect, process, or display Protected Health Information (PHI). |
| **Unauthenticated Pages** | Public-facing web pages or application screens that do not require login but may still collect or store information that can be linked to an individual, such as IP addresses or behavioral data. |
| **Online Tracking Technologies (OTTs)** | Scripts, pixels, tags, or SDKs embedded in websites or mobile apps that collect and transmit information about user interactions, behavior, or device activity. |
| **IIHI / PHI / ePHI** | • IIHI (Individually Identifiable Health Information): Any information that can be used to identify an individual in connection with their health status, care, or payment.<br>• PHI (Protected Health Information): IIHI that is created, received, maintained, or transmitted by a HIPAA-covered entity.<br>• ePHI (Electronic Protected Health Information): PHI that is stored or transmitted in electronic form. |
| **Business Associate Agreement (BAA)** | A legally binding agreement between a regulated entity and a vendor that governs how Protected Health Information is handled. A BAA ensures that any third party processing PHI adheres to HIPAA's privacy and security requirements. |
| **Consent and Preference Management (C&P)** | The processes and technologies used to collect, manage, and enforce a user's choices regarding how their data is collected, used, and shared across digital experiences. This typically includes consent banners, preference centers, and Consent Management Platforms (CMPs). While these tools define and record user intent, they do not guarantee that third-party technologies behave accordingly at runtime—making validation through mechanisms such as a Consent Audit essential for true compliance. |