HIPAAtrek

HIPAA and Beyond: The New World of Privacy and Security

May 7, 2025

Someone to Lava (HIPAA Parody)

A long, long time ago, well exactly a year ago,
I stood up here and told ya, HIPAA's gonna change.
In 2024, we had six changes,
Mostly affecting Information Blocking.
I promised that the OCR would be changing even more, in fact, it will be changing
For years and years.

Chorus: I have a dream I hope will come true,
That I can comply with HIPAA and HIPAA stops changing.
I wish I had some time to get through my HIPAA to-do's,
Stop sending me something to HIPAA.

I hear ya, I know you need a break from all the change,
And you might be on the brink of quitting.
But little do you know that this year's changes
Will mainly be for IT!

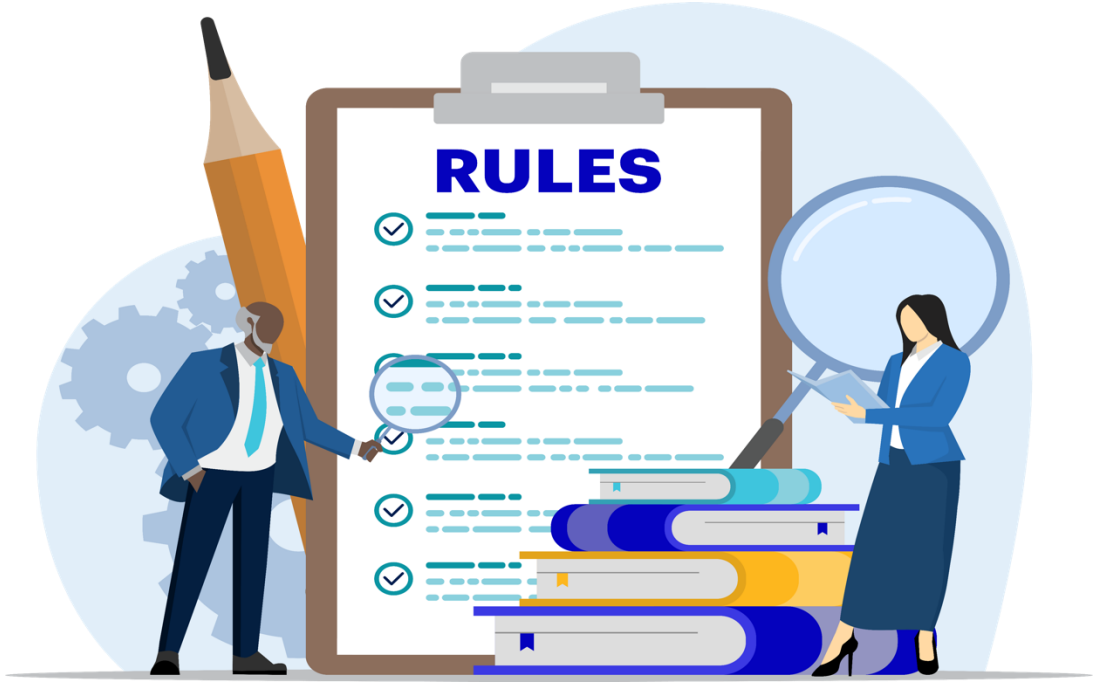
The Security Rule has never changed; that is, until now,
Because the OCR is tired of all these breaches.
But don't think Privacy is quite out of the dark,
We still have more Privacy changes coming too.

Chorus

Before you complain too much about all these changes,
Without them, I wouldn't be up here singing this amazing song.
Because these rule changes are coming way too fast,
It's also an opportunity for even more HIPAA fun.

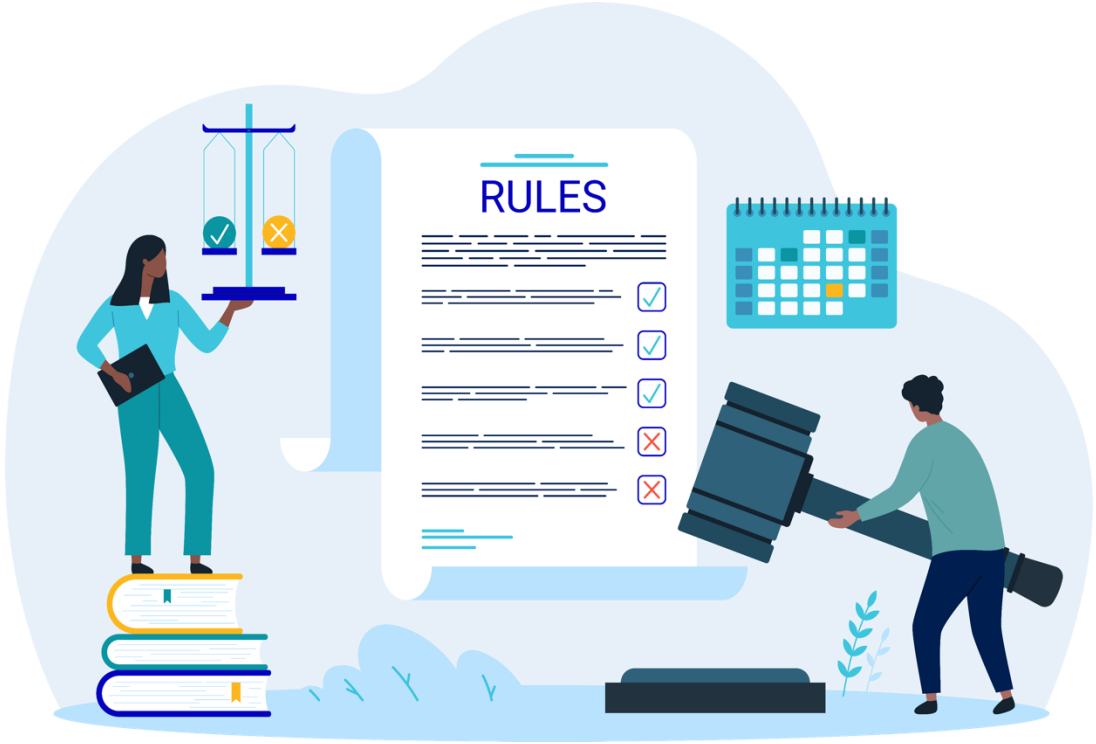
I had a dream I knew would come true,
That you would like this song so much that you are happy about all the change.
I want to thank the OCR for all of these changes,
I HIPAA You! (x3)

Importance of Privacy & Security in Healthcare



- Protects Patient Confidentiality
- Prevent Data Breaches
- Ensures Compliance
- Maintains Trust
- Supports Data Integrity
- Prevents Financial & Legal Risks
- Enhances Patient Care

Regulatory Environment



- **Regulatory Changes:** Multiple updates last year with more expected annually.
- **Why the Change?:** Healthcare is the most breached industry, compromising patient safety.
- **Staying Ahead:** Healthcare often struggles with privacy and security best practices, but your organization does not have to follow that trend.

Regulatory Landscape

Published Final Rules	
Health Data: Certification, Transparency, & Sharing (HTI-1)	**Published:** January 2024 **Compliance Date:** March 11, 2024
Substance Use Records Confidentiality (42 CFR Part 2)	**Published:** February 2024 **Compliance Date:** February 16, 2026
HIPAA: Reproductive Health Privacy	**Published:** April 22, 2024 **Compliance Date:** December 23, 2024
Information Blocking Disincentives for Providers	**Published:** July 1, 2024 **Compliance Date:** July 31, 2024
Health Data: TEFCA (HTI-2)	**Published:** December 14, 2024 **Compliance Date:** January 15, 2025
Health Data: Protecting Care Access (HTI-3)	**Published:** December 17, 2024 **Compliance Date:** December 17, 2024

Proposed Rules	
Health Data: Engagement, Info Sharing, Public Health ('HTI')	**NPRM Published:** July 17, 2024 **Final Action:** March 2025
HHS: Health IT Standards	**NPRM Published:** August 9, 2024 **Final Action:** June 2025
Telecom Relay & Info Sharing for Uniformed Services	**NPRM Published:** January 21, 2021 **Final Action:** September 2025
CIRCIA Reporting Requirements	**NPRM Published:** April 4, 2024 **Final Action:** October 2025
Modifications to the HIPAA Privacy Rule	**NPRM Published:** January 21, 2021 **Final Action:** November 2025
Security Rule: Strengthening Cybersecurity for ePHI	**NPRM Published:** January 6, 2025
Non-Discrimination for SUD Records	**NPRM Publication:** November 2025
HITECH Act: Implementation Provisions	**NPRM Publication:** May 2026

Privacy & Security: Partners in Compliance

Privacy and Security are Interdependent:

- **Privacy** protects patient PHI and controls access.
- **Security** safeguards PHI from unauthorized access, loss, or theft.

You can’t have privacy without security:

- Weak security measures expose PHI to unauthorized access, violating privacy.

You can’t have security without privacy:

- Strong security is useless if PHI is shared improperly or without authorization.

Both are necessary:

- **Security** is the lock, and **Privacy** is the rule about who has the key.

Elevating Privacy and Security in Healthcare

More Than Following Regulations:

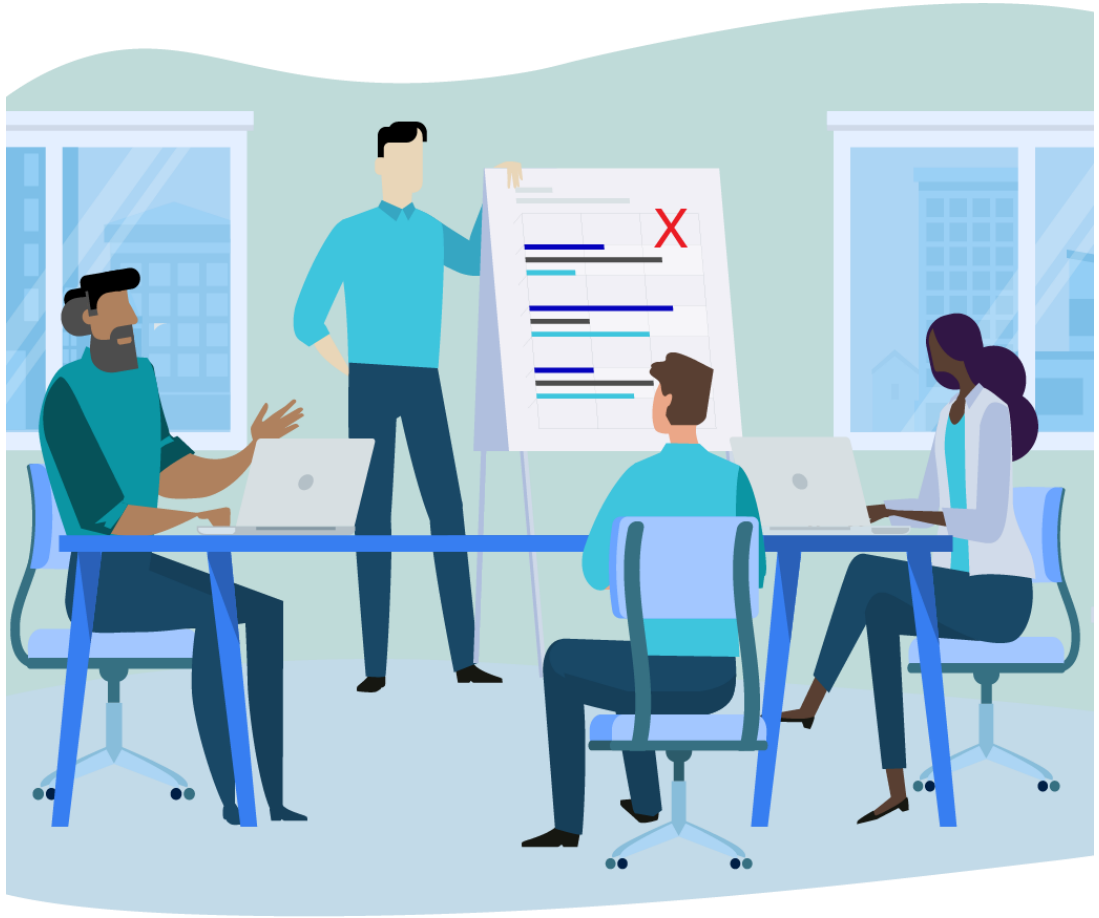
- Guides organizational practices & decision-making
- Defines culture, ethics, & values
- Protects patients – ransomware has led to documented patient deaths; privacy & security are essential to patient care.

More Than "Just" HIPAA:

- Multiple regulatory agencies are now in the privacy & security space
  - ATSP/ONC (Assistant Secretary for Technology Policy/Office of the National Coordinator)
  - SAMHSA (Substance Abuse and Mental Health Services Administration)
  - CISA (Cybersecurity and Infrastructure Security Agency)
  - OCR (Office of Civil Rights)

Proactive Approach

- Prevention is Key!
- Protects Patient Safety
- Reduces Financial & Legal Consequences
- Builds Patient Trust
- Ensures System Resilience
- Regulatory Compliance
- Future-Proofing



Strategy and Planning is Key

- **Danger of the Checklist Mentality**
- **Looking Ahead: Beyond Tech Stack and Regulations**
- **Involvement of Board and Senior Leadership**
- **Incorporating Compliance into Everyday Workflows**
  - Engaging Employees: Posters & Hallway Conversations
  - Get Out of the Office (“GOO”)
  - Technology as a Compliance Enabler

What Your Compliance Action Plan Needs to Succeed in 2025

- A compliance action plan is more than a static document — it's a **living**, evolving framework.
- It needs to be adaptable to shifting regulatory requirements and emerging risks.
- A solid action plan includes:
  - Regulatory priorities and risks
  - Assigned responsibilities
  - Routine activities and trigger-based tasks
  - A method for documenting and tracking compliance actions

From Plan to Practice: Turning Your Compliance Plan Into Action

HIPAA policies isn't the same as **doing** what they say

"HIPAA compliance" isn't just a binder on a shelf

A plan without action is just…paperwork

OCR doesn't want promises—they want **proof**

The real risk? Thinking you're compliant when you're not

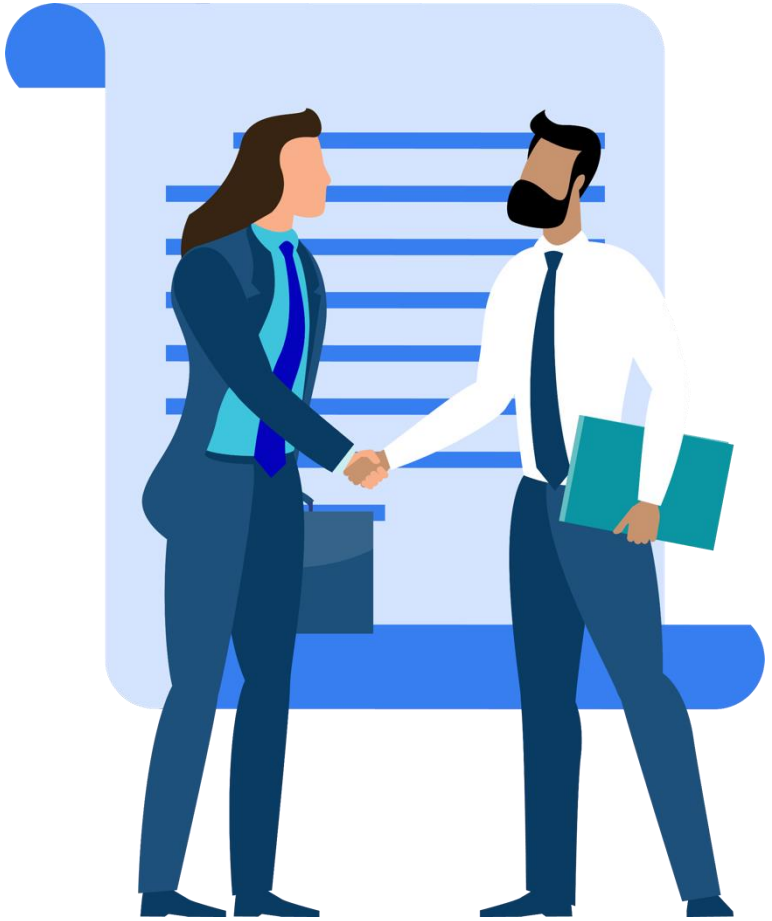
Implementation is where protection — and peace of mind — begin

Integrated Compliance Teams

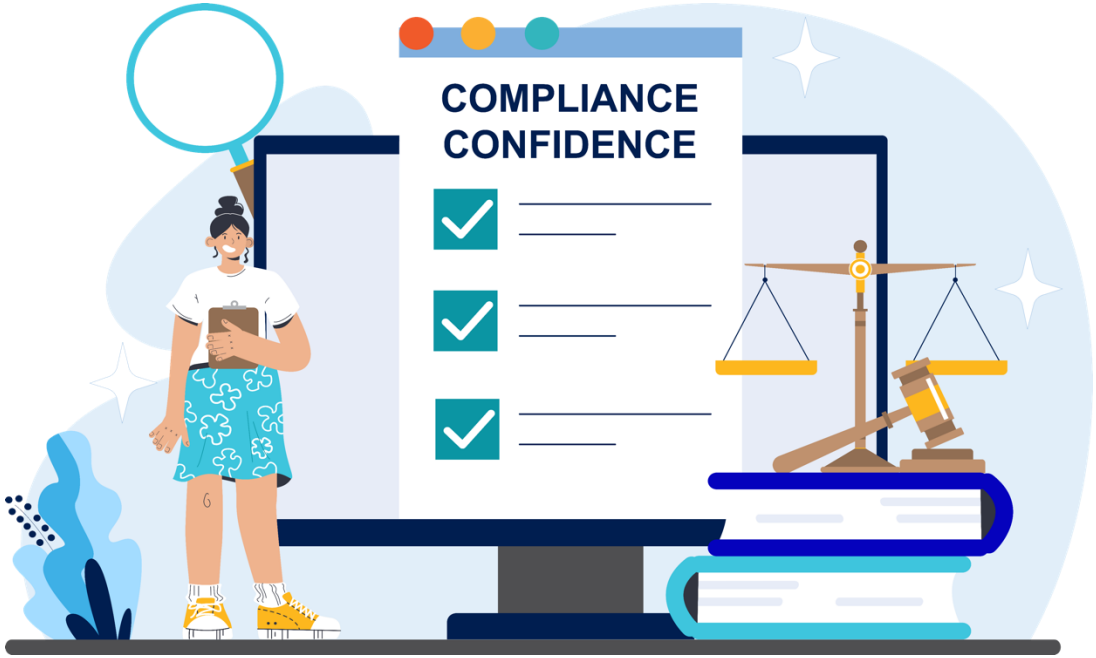
- **Organization-Wide Responsibility**
- **Diverse Compliance Teams:**
  - Includes representatives from HIM, IT, Clinical, Financial, HR, Maintenance, and Senior Leadership
- **Size of the Team Varies:**
  - Some activities need larger teams, other may only need a few reps.
- **Integration with Other Teams:**
  - Compliance can be embedded in other areas, like Hospital Incident Command or SIRT for ransomware response.

Winning Leadership Support for Compliance Initiatives

- Danger of “Status Quo is Good to Go”
- Financial Impact of Non-Compliance
- HIPAA Framework
- Proactive vs. Reactive
- Leadership’s Budget Focus
- Cyber Insurance



Ensuring Compliance Year-Round



- Annual reviews are the floor—not the ceiling
- Regulatory expectations are shifting—fast
- What passed last year may fail this year
- Policies drift over time—risk grows silently
- Regulatory risk assessments catch issues **before** they become exposures
- Staying compliant means staying current

“Dock of the Bay” (HIPAA Parody)

Sittin’ here hangin’ my head,
I’ll be sittin’ here cryin’ soon,
Watchin’ HIPAA grow,
I’ll watch my sanity shrink.

Sittin’ here readin’ the regs,
Thinkin' to myself 'what the heck',
I'm just sittin' here readin’ the regs,
Stressin' out.

I left my compliance meeting,
Headed for IT,
'Cause now we need to coordinate,
Still with no budget.

So, I'm just
Sittin’ here readin’ the regs,
Thinkin' to myself 'what the heck',
I'm just sittin' here readin’ the regs,
Stressin' out.

Looks like everything’s gonna change,
Privacy and Security,
I can't do what all I am supposed to do...
So maybe I’ll just quit and move to the beach.

Now I’m sittin' at home,
And this stress won't leave me alone,
Read two thousand reg pages,
Just in time for the OCR to release more.

Now, Sittin’ here readin’ the regs,
Thinkin' to myself 'what the heck',
I'm just sittin' here readin’ the regs,
Stressin' out.

HIPAAtrek

Thank you for joining us!

Any questions?

Contact us:

Sarah Badahman

Sarah@hipaatrek.com

651-467-5400 (Direct)