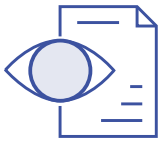
HIPAA COMPLIANCE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was established to protect patients in the U.S and improve nationwide access to and coverage for healthcare. In keeping with these objectives, regulations (outlined in the HIPAA Privacy Rule and Security Rule) were developed to protect the privacy and security of certain health information.

Today, healthcare organizations face the task of securing vast quantities of protected health information (ePHI) while also maintaining data accessibility for healthcare professionals who need it. Since data is shared across many unique networks, platforms, electronic health records (EHRs) and databases, it is crucial to understand exactly where ePHI and PII are located. Healthcare organizations have an obligation to their patients, community, partners and their own organizations to maintain HIPAA compliance and prevent health data breaches.

Ground Labs provides leading-edge data discovery solutions to healthcare organizations worldwide, helping them maintain HIPAA compliance while enabling better, more efficient patient care. Operate with confidence that your ePHI is managed across all platforms, networks, and operating systems – from pharmacy, laboratory systems, administrative networks, and third-parties.

HOW GROUND LABS CAN HELP ENSURE HIPAA COMPLIANCE

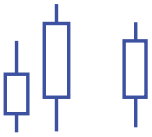


Identify over 300 predefined and variant types of data, including HIPAA-protected data stored in servers, on desktops, email, and databases, on prem and in the cloud.

Access data discovery support for HIPAA-specific data types including patient PII and national insurance identifiers, and easily set up custom parameters for medical identifiers.

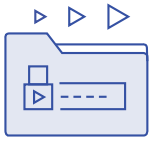
Upon a possible breach, fulfill the HIPAA Security Incident Procedures requirement by implementing sensitive data discovery & identification processes.

Gain deeper visibility across your entire enterprise, including data stored in the cloud, to pick up on and protect against potential insider and outsider threats.

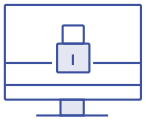


Demonstrate HIPAA compliance with fully customizable analytics & reporting, indicating the location of sensitive data and the measures taken to protect it.

Allow third-party vendors to generate evidence of safe ePHI and PII storage practices by extending access through an API Framework.



Enable faster and deeper implementation of HIPAA policies & procedures to prevent and contain security violations.



Easily build custom data types and search platforms to locate and remediate unique data types to address your organization's unique HIPAA needs.

Book a complimentary sample data analysis with Ground Labs at
https://go.groundlabs.com/book-a-demo

GROUND LABS

BOOST YOUR HEALTHCARE DATA PRIVACY WITH MODERN DISCOVERY TOOLS

Over the past decade, the U.S. healthcare industry has shifted to digital record keeping, which has raised concerns about privacy and where sensitive healthcare data is stored.

Today, health-related information spans far beyond the walls of a medical facility — in fact, it's stored and shared through fitness apps, mental health programs, and telehealth services, all of which have surged in use since the onset of COVID-19. As the volume of healthcare data being shared day to day grows exponentially, the limits of the HIPAA framework feels limiting. Given the evolving healthcare landscape, how can clinicians and practitioners maintain HIPAA compliance and make data privacy in healthcare a top priority?

What is Healthcare Data & Why Does It Matter?

Healthcare data is both extremely sensitive and valuable. This type of data can range to past health history, such as treatments and medications, to health insurance data, which often contains Social Security numbers, addresses, employer information, and more.

According to a recent TrustWave survey, the value of health data was found to be around $250 per record. Additionally, IBM found that a data breach in the healthcare industry costs, on average, $6.45 million and the impact on an individual can be emotionally damaging.

Last year, the healthcare sector saw a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking, according to the Protenus Breach Barometer. And this year's figures look to be equally, if not more, disturbing, especially amid the global pandemic which has forced the healthcare industry into digital transformation overdrive.

Put Healthcare Privacy First with Ground Labs

Trusted by top healthcare organizations, Ground Labs' award-winning solution, Enterprise Recon, has the ability to discover over 300 predefined and variant types of data, including healthcare IDs and insurance information.

With Enterprise Recon, organizations can discover and remediate data across a variety of locations, including healthcare information stored on servers, on personal desktops, in the cloud and more. Ground Labs is designed to ensure HIPAA compliance, allowing any organization that handles healthcare data to maintain consumer privacy and be a good steward of customer trust.

HOW CAN HEALTHCARE PROFESSIONALS PUT PRIVACY FIRST?

Given the evolving nature of data, the privacy of healthcare can become complicated in regard to its collection, where it goes, and how it's used in the future. But healthcare professionals can prioritize privacy by following a few simple measures:

- **Understand HIPAA rules and regulations**: enacted in 1996, the law focuses on portability (Title I) and administrative simplification (Title II). The portability portion of the law was enacted to ensure health insurance portability between jobs. Understanding the intricacies of HIPAA, including patients' rights as well as what type of data is covered, is the first step to gaining a better grasp on privacy.
- **Implement processes to cover the entire lifecycle of healthcare data**: organizations that handle healthcare data must install safeguards that cover data collection, governance and handling.
- **Leverage data discovery**: Data discovery technologies can help organizations derermine where sensitive healthcare data resides. Gaining this understanding will help determine where the problem resides, and ensure security measures are in place to protect privacy.