Compliancy Group

Lessons From

DATA BREACHES & FINES

LEARN ABOUT COMPLIANCE RISKS AND WHAT TO EXPECT IN 2025.

HHS ISSUED $9 MILLION IN FINES

In 2024, the Department of Health and Human Services (HHS) Office for Civil Rights settled **sixteen** cases with healthcare organizations for potential HIPAA violations.

Fines ranged from **$35,000 - $4.75 million**, totaling **$9,164,206**.

Which Entities Were Fined?

1. Montefiore Medical Center: **$4.75M**
2. Gulf Coast Pain Consultants: **$1.19M**
3. Heritage Valley Health: **$950K**
4. Children's Hospital of Colorado: **$548K**
5. Plastic Surgery Associates of SD: **$500K**
6. Inmediata Health Group, LLC.: **$250K**
7. Cascade Eye & Skin Centers: **$250K**
8. Providence Medical Institute: **$240K**
9. American Medical Response: **$115K**
10. Hackensack Meridian Health: **$100K**
11. Rio Hondo Community Mental Health Center: **$100K**
12. Bryan County Ambulance Authority: **$90K**
13. Gums Dental Care: **$70K**
14. Green Ridge Behavioral Health: **$40K**
15. Phoenix Healthcare: **$35K**
16. Holy Redeemer Family Medicine: **$35K**

Risk Analysis Enforcement

Montefiore Medical Center: $4.75M

Patient information had been stolen from the hospital's database in an inside job. For six months, the **employee stole patient PHI** and sold it to an identity theft ring.

Gulf Coast Pain Consultants: $1.19M

A terminated contractor accessed the **ePHI of 34,310 individuals**. The contractor then filed medical claims for services that were not actually rendered, resulting in approximately **6,500 false Medicare claims**.

Children's Hospital of Colorado: $548K

In two separate incidents, employees fell prey to **phishing incidents,** allowing hackers to access their accounts. The PHI of **10,840 patients** was compromised.

Inmediata Health Group, LLC.: $250K

A database of **1.5 million patients** was left unsecured on the Internet –findable through search engines like Google.

Double Trouble

Risk Analysis & Ransomware

Heritage Valley Health: $950K

Compliance review initiated after the **media reported** that HVHS experienced a ransomware attack.

Plastic Surgery Associates of South Dakota: $500K

Nine workstations and two servers were infected with ransomware. They **paid hackers 2 Bitcoin** for the return of patient files.

Cascade Eye & Skin Centers: $250K

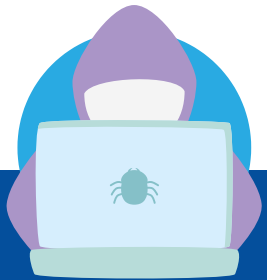
Suffered a ransomware affecting **291,000 patients**.

Bryan County Ambulance Authority: $90K

14,273 patient records were encrypted in a ransomware incident.

Green Ridge Behavioral Health: $40K

Hackers who broke into their server encrypted **14,000 patient files**.



"Risk analysis—for those of you who live and breathe this—understand it's a requirement under the HIPAA Security Rule. If you look at any of our enforcement work online, literally any of the cases in our press releases, risk analysis is four out of five times one of the elements that is flagged in those enforcement actions because it is not being prioritized. It is not being done in the right way," said OCR Director Melanie Fontes Rainer.

So far OCR has settled **four cases** under their new **Risk Analysis Enforcement Initiative** and is likely to ramp up efforts in the next couple of years.

In November 2023, OCR settled its first **Ransomware** settlement, and as of January 2025, has already settled **10 cases**.

Right of Access Fines

American Medical Response: $115K

Rio Hondo Community Mental Health: $100K

Essex Residential Care, LLC: $100K

Gums Dental Care: $70K

Phoenix Healthcare: $35K

> "An essential hallmark of HIPAA is the right to patients' timely access to their medical records. Patients should not have to make multiple requests and file complaints with HHS' Office for Civil Rights to get their own medical records," said **OCR Director Melanie Fontes Rainer**.

The Outliers

While **Providence Medical Group** settled for **$249K** under the Ransomware Initiative, they were the only organization that was not flagged for a lack of Risk Analysis. Their compliance failure stemmed from **failing to limit access to PHI**, and a **lack of BAA** with their business associate.

Holy Redeemer settled **$35K** for a unique Privacy Rule violation having impermissibly disclosed PHI to a patient's prospective employer.

DOJ HEALTHCARE FRAUD STRIKE FORCE

In a two-week operation, **193 people** were charged in **145 cases** involving more than **$2.75 billion** of intended losses and **$1.6 billion** in actual losses.

76 charged were licensed healthcare providers in cases involving medically unnecessary amniotic wound grafts, diverted HIV medications, online distribution of Adderall, and other telemedicine schemes.

False Claims Act Violations Billing Fraud

Rite Aid Corporation: $121M
Inaccurately reporting drug rebates to Medicare.

Walgreens: $106.8M
Allegations of billing government programs for prescriptions that were processed and never picked up.

Acadia Healthcare Company: $16.6M
Allegations of billing for unnecessary services, improper discharges and staffing shortcomings.

> "The Department places a high priority on fighting fraud and abuse in federal programs. Such conduct will not be tolerated, and that those who knowingly misuse taxpayer funds will be held accountable," said **Principal Deputy Assistant Attorney General Brian Boynton, head of the DOJ's Civil Division.**

False Claims Act Violations Illegal Referrals

Community Health Network: $345M
Allegations of claims submitted to Medicare for services referred in violation of the Stark Law.

Oak Street Health: $60M
Allegations of kickback payments to third-party insurance agents in exchange for recruiting seniors to its clinics.

DaVita: $34.5M
Allegations of kickbacks paid to a competitor to induce referrals.

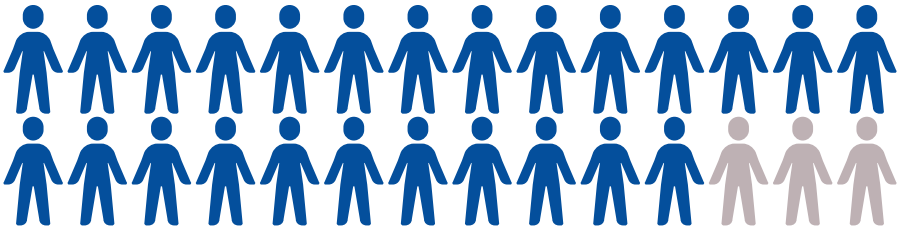
Settlements totaled $1.7B in 2024

2024 FINES FACTS AND LESSONS

- FAILURE TO CONDUCT A RISK ANALYSIS CAN COST YOU BIG!
- RANSOMWARE SETTLEMENTS ARE A MAIN FOCUS
- OCR IS STILL ENFORCING THE HIPAA RIGHT OF ACCESS
- DON'T FORGET ABOUT THE FALSE CLAIMS ACT
- EMPLOYEES ARE STILL FALLING VICTIM TO PHISHING SCHEMES
- LIMITING WHO CAN ACCESS PHI IS OF UTMOST IMPORTANCE

2024 Reported Breaches

The OCR breach portal also listed **580** large-scale breaches on its site



177,467,758 patients affected by healthcare breaches in 2024

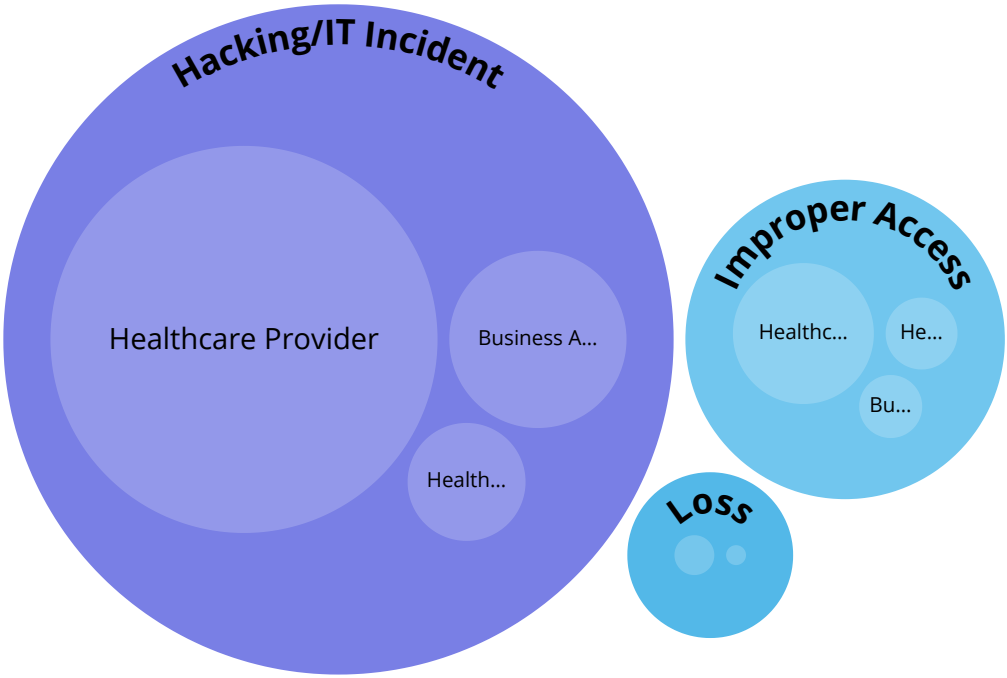
42% increase from 2023's **124.6 million** patients

"Cyberattacks continue to impact the healthcare sector, with rampant escalation in ransomware and hacking causing significant increases in the number of large breaches reported to OCR annually," OCR Director Melanie Fontes Rainer.

Since 2018, there has been a **264%** increase in breaches involving hacking ransomware.

In 2024, there were **161.5 million patients** affected by hacking, accounting for **91%** of the large breaches reported to OCR. **114** of those incidents were reported as phishing, emphasizing the need for not only risk analysis, but employee cybersecurity training.

What Type of Incidents Were Reported?



73

Improper Access or Disclosure

492

Hacking Incidents

8

PHI Theft

Who Reported Breaches

440

Healthcare Providers

91

Business Associates

48

Health Plans

1

Healthcare Clearinghouse

Patients Affected by Breaches

91%

of patients affected were due to hacking or IT incidents.

8.9%

of patients affected were due to unauthorized access or disclosure of PHI.

0.02%

of patients affected were due to theft, loss, or improper disposal of PHI.

Preventing Breaches and Fines in Healthcare

As breaches targeting healthcare organizations skyrocket, it is essential to implement measures to prevent unauthorized access to sensitive data.

Implementing an effective HIPAA compliance program is the best way to do so. HIPAA compliance includes risk analysis, policies and procedures, employee training, and incident management. Had organizations fined by OCR over the last year implemented an effective compliance program, the incident and subsequent fine could have been prevented.

EFFECTIVE HEALTHCARE COMPLIANCE PROGRAM

- IMPLEMENT POLICIES, PROCEDURES, AND STANDARDS OF CONDUCT
- DESIGNATE A COMPLIANCE OFFICER AND COMPLIANCE COMMITTEE
- CONDUCT EFFECTIVE TRAINING AND EDUCATION
- DEVELOP EFFECTIVE LINES OF COMMUNICATION
- CONDUCT INTERNAL MONITORING AND AUDITING
- ENFORCE STANDARDS THROUGH WELL-PUBLICIZED DISCIPLINARY GUIDELINES
- RESPOND PROMPTLY TO DETECTED OFFENSES AND UNDERTAKE CORRECTIVE ACTION

Compliancy Group's Compliance Software

Snapshot of Compliance Status
Easily view your current compliance status and task list.

Employee Training
Effectively assign employee training, and track their progress.

Policies and Procedures
Create custom policies and procedures that meet compliance needs.

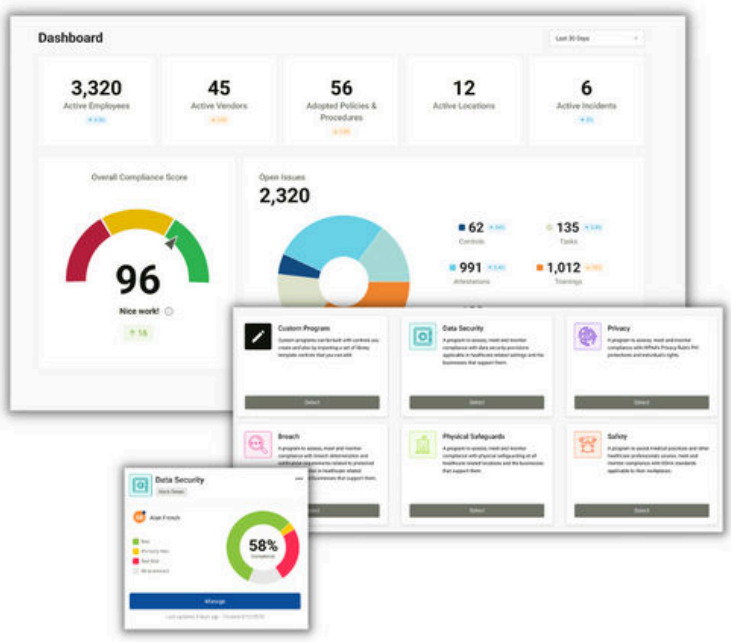
Risk Assessments
Simply answer a series of yes or no questions to assess your risk.

Corrective Actions
Get corrective action plans automatically assigned based on answers.

Incident Management
Easily report, track, and manage incidents.

There is a lot that goes into a healthcare compliance program, and our solution helps automate the process. Whether you need HIPAA, OSHA, SOC 2, or other regulatory requirements, your compliance program is fully customizable.

Compliancy Group's Compliance Software



Compliancy Group is the leading all-in-one healthcare compliance solution. Our intuitive software simplifies regulatory complexities, helping thousands of organizations confidently track and manage compliance. With a 100% audit pass rate, we deliver real, measurable outcomes so you can focus on what matters most—providing exceptional care.

Our software encompasses all essential compliance features: templated policies and procedures, risk assessments, comprehensive training for your entire team, vendor management, incident reporting, and much more. Whatever your needs, our platform offers guided action items to effortlessly meet your requirements.

Eliminate the complexities and stress associated with compliance, enhance patient loyalty, and minimize risk. Supported by leading medical associations, clients can trust in the strength of their compliance program.

Contact Us

Compliancy Group

855-854-4722

compliancygroup.com

info@compliancygroup.com