Compliancy Group

Lessons Learned
2023 BREACHES AND FINES

FIND OUT HOW TO PREVENT HEALTHCARE BREACHES AND FINES.

HHS ISSUED $4 MILLION IN FINES

In 2023, the Department of Health and Human Services (HHS) Office for Civil Rights settled **thirteen** cases with healthcare organizations for potential HIPAA violations.

The HHS OCR settled cases with **eight** covered entities and **four** business associates. Fines ranged from **$15,000 - $1.3 million**, totaling **$4,176,500**.

Which Entities Were Fined?

1. **LA Care Health Plan:** $1,300,000
2. **Banner Health:** $1,250,000
3. **Lafourche Medical Group:** $480,000
4. **MedEvolve:** $350,000
5. **Yakima Valley Memorial Hospital:** $240,000
6. **Optum Medical Care of New Jersey:** $160,000
7. **St. Joseph's Medical Center:** $80,000
8. **United Healthcare:** $80,000
9. **iHealth Solutions:** $75,000
10. **Manasa Health Center:** $30,000
11. **Life Hope Labs:** $16,500
12. **David Mente, MA, LPC:** $15,000

HIPAA Security Rule Violations

LA Care Health Plan suffered a breach in which **1,498** patients were affected. Since they failed to conduct an organization-wide risk analysis, implement policies and procedures, and lacked adequate security controls, they were fined.

Banner Health suffered a hacking incident in which **2.81 million** were affected. Since Banner Health failed to conduct an accurate and thorough risk analysis, implement sufficient procedures to regularly review records of information system activity, and implement technical security measures, they were fined.

HIPAA Security Rule Violations

Lafourche Medical Group suffered a phishing incident in which **34,862** patients were affected. Since they failed to conduct a security risk assessment (SRA) and lacked policies and procedures to regularly review information system activity, they were fined.

MedEvolve suffered a network server incident in which a data file was inadvertently placed on a file transfer server that was separate from their client hosting environment. Since they failed to conduct SRA and enter into a business associate agreement (BAA) with a subcontractor, they were fined.

iHealth Solutions filed a breach report indicating an unauthorized transfer of protected health information (PHI) from an unsecured server occurred. Since they failed to conduct a thorough SRA and have a risk management plan, they were fined.

Right of Access Fines

Optum Medical Care failed to provide timely access to medical records to six patients.

UnitedHealthcare failed to provide timely access to a patient’s medical records.

Life Hope Labs failed to provide timely access to the medical records of a deceased patient to their personal representative.

David Mente, MA, LPC, failed to provide timely access to the medical records of a minor patient to their personal representative.

Unauthorized Access or Disclosure Fines

Yakima Valley Memorial Hospital suffered an insider breach in which 23 security guards used their login credentials to access patient electronic protected health information. Due to a lack of policies, procedures, and access controls, Yakima was fined.

St. Joseph's Medical Center disclosed patient information to a news reporter without consent. As a result, they were fined, and must amend their policies and procedures, and retrain their workforce on the new guidelines.

Manasa Health Center impermissibly disclosed PHI in response to a patient's negative online review. As a result, they were fined, and must amend their policies and procedures, and retrain their workforce.

2023 FINES FACTS AND LESSONS

☑ HIPAA SECURITY RULE VIOLATION FINES REIGNED SUPREME

☑ THE HIPAA RIGHT OF ACCESS INITIATIVE REMAINED A TOP PRIORITY

☑ DOCTORS OFFICES MUST LEARN HOW TO RESPOND TO PATIENT REVIEWS

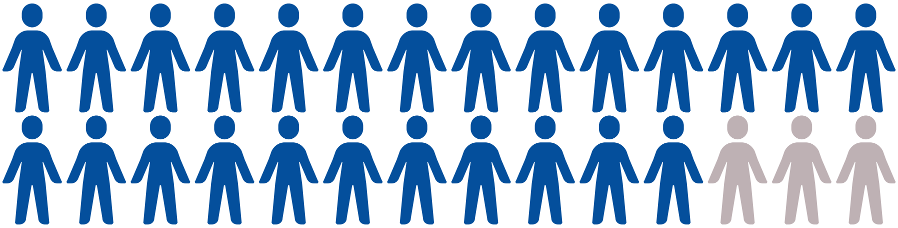
☑ INSIDER BREACHES REMAIN A THREAT

☑ HACKING AND PHISHING HAPPEN, BUT WHEN YOU DON'T CONDUCT AN SRA YOU'LL BE FINED

☑ BUSINESS ASSOCIATE AGREEMENTS ENSURE YOUR VENDORS UPHOLD HIPAA STANDARDS

2023 Reported Breaches

The OCR breach portal also listed **563** large-scale breaches on its site



124,630,800 patients affected by healthcare breaches in 2023

127% increase from 2022’s **55 million** patients

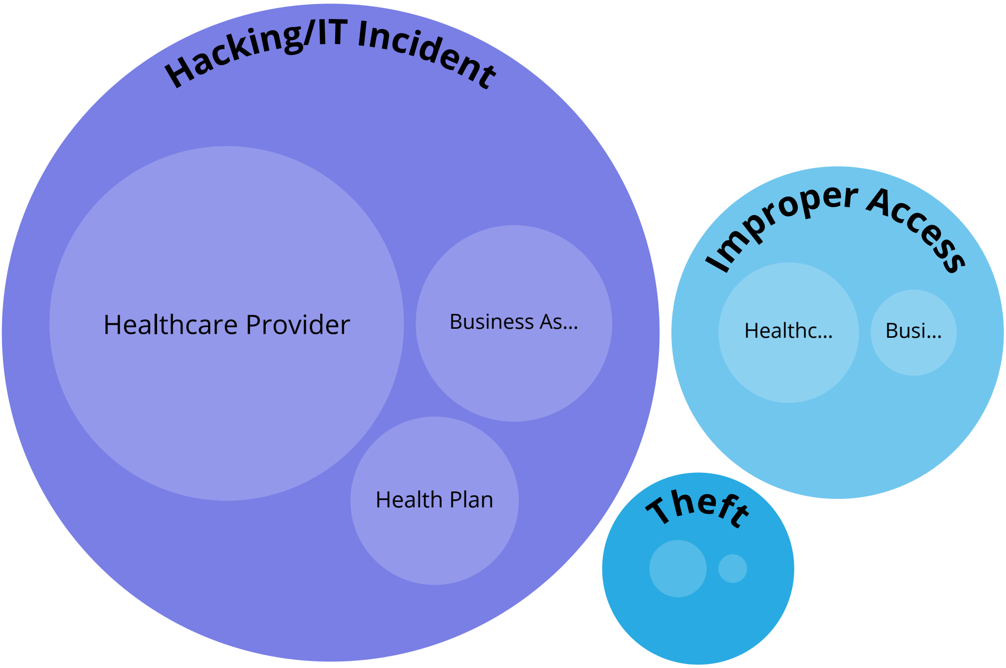
Ransomware attacks are increasingly common and targeting the health care system. This leaves hospitals and their patients vulnerable to data and security breaches." said OCR Director, Melanie Fontes Rainer.

In this ever-evolving space, it is critical that our health care system take steps to identify and address cybersecurity vulnerabilities along with proactively and regularly review risks, records, and update policies. These practices should happen regularly across an enterprise to prevent future attacks.

Over the past four years, there has been a **239%** increase in breaches involving hacking and a **278%** increase in ransomware.

In 2023, hacking accounted for **84%** of the large breaches reported to OCR.

What Type of Incidents Were Reported?



77

Improper Access
or Disclosure

472

Hacking
Incidents

10

PHI
Theft

Who Reported Breaches

366

Healthcare Providers

115

Business Associates

80

Health Plans

2

Healthcare Clearinghouse

Patients Affected by Breaches

93.4%

of patients affected were due to hacking or IT incidents.

6.5%

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

0.017%

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

Compliancy Group

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.

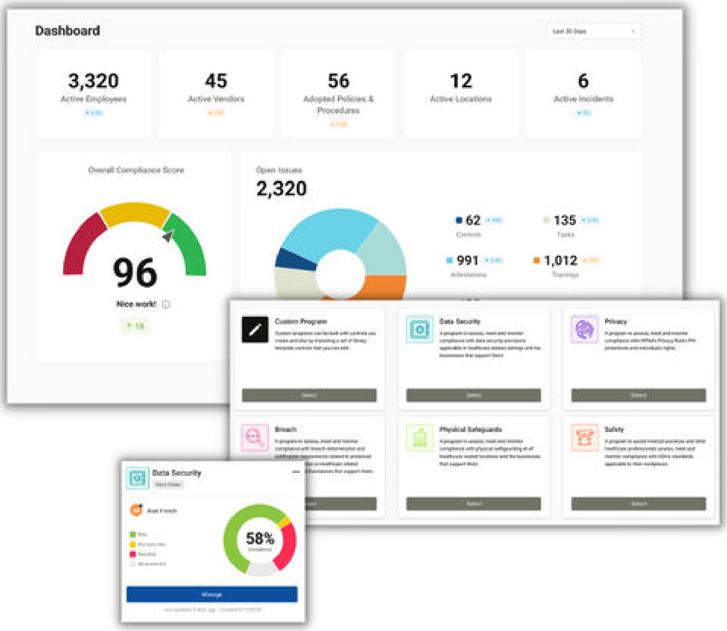
Risk Assessments
Simply answer a series of yes or no questions to assess your risk.

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



Our software has everything you need for compliance: templated policies and procedures, risk assessments, comprehensive training for your entire staff, vendor management, incident reporting, and more. No matter your needs, our software provides guided action items to meet your requirements with ease.

Solve healthcare compliance challenges quickly and confidently with simplified software. Remove the complexities and stress of compliance, increase patient loyalty and the profitability of your business, and reduce risk. Endorsed by top medical associations, clients can be confident in their compliance program.

Get compliant today!

Contact Us

Compliancy Group

☎ 855-854-4722

compliancygroup.com

✉ info@compliancygroup.com