Page Title: HIPAA Horror Stories: Violation Examples and Cases (2025) | imageOne

HIPAA Horror Stories: HIPAA Violation Examples and Cases (2025)

In today's digital age, safeguarding protected health information (PHI) and complying with the Health Insurance Portability and Accountability Act (HIPAA) present significant challenges. With cybersecurity threats on the rise and mounting concerns about patient data privacy, healthcare organizations must be vigilant about system vulnerabilities, printer security mistakes, and document workflow lapses that can lead to serious breaches and violations.

This article will cover common examples of HIPAA violations, some of the biggest HIPAA violation cases, and best practices for securing your printers and document workflows.

- Common Examples of HIPAA Violations
- 10 Famous HIPAA Violation Cases
- Are Your Printers HIPAA Compliant?
- Best Practices for HIPAA-Compliant Printing

Protect patient privacy with secure print management for the healthcare industry from ImageOne.

Examples of Common HIPAA Violations in Healthcare

The **Health Insurance Portability and Accountability Act (HIPAA)** sets national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Despite these clear guidelines, however, HIPAA violations still occur regularly—sometimes due to negligence and other times due to intentional misconduct. Common violations include:

- **Snooping: D**eliberate unauthorized viewing of medical records of friends, neighbors, family members, or others for personal reasons
- **Improper Disposal:** Failing to destroy patient records containing PHI adequately, e.g., incinerating or shredding
- **Lost or Stolen Devices:** Unencrypted data containing PHI on lost or stolen devices leading to security risks
- **Lack of Workplace Controls -** Unauthorized access to patient medical records due to careless handling, like leaving sensitive information accessible on unattended computers or paperwork left out haphazardly.
- **Delayed Breach Notification:** Failing to inform patients promptly after a breach
- **Limited patient access:** Delays or inability of patients to access their records in a timely fashion
- **Inadequate Risk Analysis:** Failing to perform regular risk assessments to uncover potential security vulnerabilities

Ensure your print environment is HIPAA compliant with Managed Print Services for Healthcare.

10 Notable HIPAA Violation Cases

Since the HIPAA Privacy Rule's implementation in April 2003, the Office for Civil Rights (OCR) has received nearly 375,000 HIPAA complaints, and civil penalties from such cases have totaled $144,878,972.

HIPAA violations occur across industries and for a number of causes, as mentioned above. Any individuals who handle or come into contact with PHI have the potential to commit a HIPAA violation that exposes sensitive patient data and puts themselves and their organization in hot legal waters.

Below, we'll cover some of the most notable real-life HIPAA violation cases to demonstrate the many ways these infractions can occur, specifically as they relate to poor document handling and printing security incidents.

1. Command Marketing Innovations, LLC & Strategic Content Imaging
2. Affinity Health Plan, Inc.
3. Centegra Data Breach
4. BeHealthy Health Plan
5. Advocate Health Care Network
6. Blue Cross and Blue Shield of Nebraska
7. Parkview Healthcare System
8. Aetna
9. CVS Pharmacy
10. Cignet Health Center

1. Command Marketing Innovations, LLC & Strategic Content Imaging, LLC, New Jersey

CMI and SCI provided printing and mailing services to a New Jersey-based healthcare organization.. In the fall of 2016, a printing error resulted in these companies inadvertently mailing out to the wrong patients sensitive data that included claims numbers, descriptions of services, provider names, and other details. Earlier in the year, SCI had changed its printing processes, causing the last page of one patient's statement to be sent to the next person.

An investigation by the New Jersey Division of Consumer Affairs determined that the disclosure of the PHI violated HIPAA laws under the printing providers' business associate agreement with the healthcare organization and that CMI and SCI failed to review benefits statements before mailing them out.

- **Cause**: Poor workflow controls
- **Individuals impacted**: 55,715
- **Settlement cost**: $130,000

imageOne specializes in document workflows to meet healthcare standards, including HIPAA.

2. Affinity Health Plan, Inc., New York

Printing error resulted in sensitive data being mailed incorrectly

Affinity Health Plan, Inc. leased a photocopier with an internal hard drive that stored copies of documents including patient medical records. Affinity returned the photocopier to the leasing company without erasing the stored data. CBS Evening News subsequently purchased the device, discovered the stored records, and reported the breach to Affinity.

An OCR investigation found that Affinity disclosed PHI to unauthorized individuals, violating HIPAA compliance by failing to delete the stored records from the hard drive before returning the device to the leasing agent. In addition to a settlement topping $1.2 million, Affinity was responsible for recovering any other photocopiers it had used and returned to the leasing company without erasing the hard drive.

- **Cause**: Improper digital records disposal
- **Individuals impacted**: 344,579
- **Settlement cost**: $1,215,780

3. Centegra Health System, McHenry County, Illinois

Failure to erase a leased copier's hard drive led to exposure of PHI
Centegra Health System contracted MedAssets, a third-party vendor, to mail patient billing statements. In 2015, a MedAssets employee made an error when configuring the mailing system that resulted in patients receiving two documents in the envelope—one that was their own billing statement and a second that was meant for another patient.

Though an accidental mistake, the mailing error exposed the PHI of thousands of patients, including mailing addresses, account numbers, service summaries, amounts owed, and more. As a result, Centegra hired a new vendor to handle mailings, and all affected patients were offered a free year of credit monitoring services.

- **Cause**: Poor workflow controls
- **Individuals impacted**: 2,929
- **Settlement cost**: Unknown

4. BeHealthy Health Plan, Manatee & Sarasota County, Florida

Personal identifying information that could be used to steal a person's identity was printed on the outside of mailing envelopes.
BeHealthy Health Plan experienced serious oversight of printing and mailing practices in 2015 when health insurance claim numbers of 835 subscribers were printed on the outside of envelopes before being mailed.

Typically, exposing just one data point, like a claim number, would not be a severe issue. BeHealthy, however, used Social Security numbers of plan members in these claim numbers. Thus, these numbers, along with the patient's name and mailing address were readily available on the outside of the envelope thereby becoming a much more serious matter. All affected members were given a free year of identity theft protection services.

- **Cause**: Poor workflow controls
- **Individuals impacted:** 835

- **Settlement cost:** Unknown

5. **Advocate Health Care Network**, Alabama, Georgia, Illinois, North Carolina, South Carolina, and Wisconsin

Unsecure data on stolen computers led to major violations and an unprecedented settlement
Advocate Health Care Network faced multiple potential HIPAA compliance violations that affected more than four million patients, resulting in an unprecedented financial settlement. Issues began when four desktop computers were stolen from the organization's administrative buildings in Illinois in July 2013, with two more minor breaches occurring shortly after.

Advocate Health's failure to conduct a sufficient organization-wide risk assessment and control physical access to digital records stored in its data support center contributed to the breach. The record-high settlement of $5.55 million was, at the time, the largest ever HIPAA settlement by a single covered entity.

- **Cause**: Failure to complete organization-wide risk assessment and control access to digital records
- **Individuals impacted:** 4,029,530
- **Settlement cost:** $5,550,000

6. **Blue Cross and Blue Shield of Nebraska**, Nebraska

Printing error resulted in statements mailed to the wrong patients
In 2015, Blue Cross and Blue Shield of Nebraska discovered a printing error that resulted in dental Explanation of Benefits (EOB) statements being sent to the wrong customers. Individuals received names, ID numbers, treatment details, and claim information for other patients, violating HIPAA requirements.

- **Cause**: Poor workflow controls
- **Individuals impacted:** 1,827
- **Settlement cost:** Unknown

7. **Parkview Healthcare System**, Indiana

Medical files were delivered, unsecured and unattended
In 2009, a doctor who had worked for Parkview Healthcare System filed a data security complaint after 71 boxes containing medical files for at least 8,000 patients were delivered to his home without proper security safeguards. The boxes were left on his driveway while the doctor was away from home, putting the confidential records unattended and at risk of exposure. The OCR imposed a fine on Parkview Healthcare System and required it to develop a training program for staff pertaining to HIPAA policies and procedures.

- **Cause**: Improper security of printed patient medical records
- **Individuals impacted:** up to 8,000
- **Settlement cost**: $800,000

8. **Aetna**, United States

Patient HIV status exposed due to mailing oversight
In 2017, Aetna inadvertently exposed the HIV status of nearly 12,000 patients due to a mailing error. Previously, Aetna required members to receive HIV medications via mail-order pharmacies–a policy that was later challenged in court as discriminatory. As part of a settlement, Aetna allowed affected members to fill prescriptions at retail pharmacies and sent notification letters to those who had previously used the mail-order service. However, the envelopes used for these letters had oversized windows that revealed sensitive information, including that the member was taking HIV medications. Aetna ultimately agreed to a settlement exceeding $17 million and implemented new safeguards to prevent similar incidents in the future.

- **Cause**: Negligent printing and mailing practices
- **Individuals impacted:** 11,875
- **Settlement cost**: $17,161,200

9. **CVS Pharmacy**, United States

Improper disposal of printed records exposed PHI
CVS Pharmacy came under investigation by the OCR after media reports alleged that the retailer was improperly disposing of physical records containing PHI. More specifically, allegations included that CVS employees were disposing of old prescription labels and bottles in unsecured dumpsters, accessible by the public. To settle potential violations, CVS agreed to pay a $2.25 resolution amount and adopt a Corrective Action Plan that included strengthening its disposal policies and procedures.

- **Cause**: Improper printed records disposal
- **Individuals impacted**: Unknown
- **Settlement cost**: $2,250,000

10. **Cignet Health Center**, Maryland

Violated privacy rules by refusing patent access to their medical records
Cignet Health operated two hospitals in Prince George's County, Maryland. On 41 occasions, Cignet refused to provide patients with their medical records upon request–an explicit violation of the HIPAA Privacy Rule. Several affected patients filed complaints with the OCR, but Cignet was reportedly uncooperative throughout the investigation. When the organization finally provided 41 requested records to the Department of Justice, it also included 4,500 additional records that did not pertain to the case nor should have been disclosed.

This case marked a milestone as the first time the OCR imposed a financial penalty–rather than issuing a corrective action plan to improve internal security standards–for a violation of the Privacy Rule.

- **Cause**: Delayed patient record disclosure and improper records handling
- **Individuals impacted**: 4,500+
- **Settlement cost**: $4,300,000

Are Your Printers HIPAA Compliant?

HIPAA violations often stem from overlooked or outdated workflows—and printing and document handling often pose the biggest hidden risks. In busy healthcare environments, unsecured networks, shared printers, and inconsistent access controls can all become points of vulnerability that compromise patient privacy.

Printers pose security risks. That's why secure, HIPAA-compliant print workflows aren't just a best practice—they're essential. By implementing tools like encrypted devices, access-based printing, and real-time monitoring, healthcare organizations can significantly reduce risk, ensure compliance, and avoid costly breaches.

At imageOne, we specialize in tailoring document security strategies for healthcare teams—optimizing workflows to improve operational efficiency while safeguarding PHI to maintain full compliance with HIPAA standards.

Best Practices for HIPAA-Compliant Printing

Ensuring HIPAA compliance requires an enterprise-wide commitment to secure printing practices and safe document handling, which the following best practices can help to achieve.

Limit Physical Access to Print Devices

Place devices used to print, copy, or fax documents containing PHI in secure, restricted-access areas. For example, a printer might be kept in a locked media closet accessible only with a key card or password. In this case, only authorized personnel should be able to access the room and devices, helping to reduce the risk of unauthorized access and potential data breaches.

imageOne helps healthcare organizations implement access control tools—like key card entry and secure print release—to prevent unauthorized use and reduce security risks.

Provide Employee Training

Many HIPAA violations result from simple oversights in day-to-day tasks. Empowering your team with regular training on secure print practices, paper and digital document handling, and policy

updates helps reduce risk and reinforce a compliance-first culture. As illustrated in the cases above, It's crucial to continually highlight the importance of compliance and the damaging risks that may result from a potential violation.

Implement "Pull" Printing

Pull printing is a secure print method that ensures documents only print when an authorized user is physically present. Instead of sending a print job to one device, which prints automatically and allows anyone to access the documents, the print job is sent to a network-wide queue. When authorized users reach a device, they must enter the necessary credentials before the document prints.

As part of our Managed Print Services, imageOne configures pull printing systems that protect patient information while streamlining workflows. Schedule a discovery call to learn more.

Regularly Monitor Audit Logs

Audit logs help detect unusual print activity early. Review print device audit logs regularly, looking for any out-of-the-ordinary access patterns or unusual usage. This helps IT teams detect and spot potential breaches or violations as early as possible, supporting prompt reporting under HIPAA's Breach Notification Rule.

Sign Up for a HIPAA-Compliant Workflow Consultation

Navigating HIPAA compliance is no easy task. Healthcare companies can use a managed print strategy from an expert partner, like **imageOne**, to help maintain HIPAA compliance while streamlining printing processes.

What are the specific benefits of managed print services? The right MPS partner will take tedious and time-consuming printer management tasks off your hands, helping you build secure and more efficient print workflows. imageOne serves businesses in Ohio, Michigan, Missouri, and beyond, offering custom-tailored solutions to meet your unique needs.

Schedule a discovery call today for a free HIPAA-compliant workflow consultation with imageOne.