DATAPATROL

USE CASE

When Authorized Access Becomes a Risk: Insider Data Leakage in Healthcare

Healthcare sector handles large volumes of sensitive data, including patient records, medical images, lab results, and clinical systems. Because many staff members require legitimate access to this information, healthcare is especially vulnerable to insider related data leakage.

This use case focuses on situations where authorized users misuse their access to take sensitive data using methods that traditional security controls often cannot detect, such as screenshots, printing, or photographing screens.

By reviewing real incidents, healthcare security teams can identify gaps in user accountability, endpoint controls, helping reduce data loss incidents, meet regulatory requirements, and protect patient trust.

Incident Reports Overview

Incident 1:
Montefiore Medical Center
(New York, USA)

In 2015 at Montefiore Medical Center in New York, a hospital employee with legitimate system access was able to print sensitive information for more than 12,000 patient and sold them for $3 per copy to outside accomplices on daily basis.

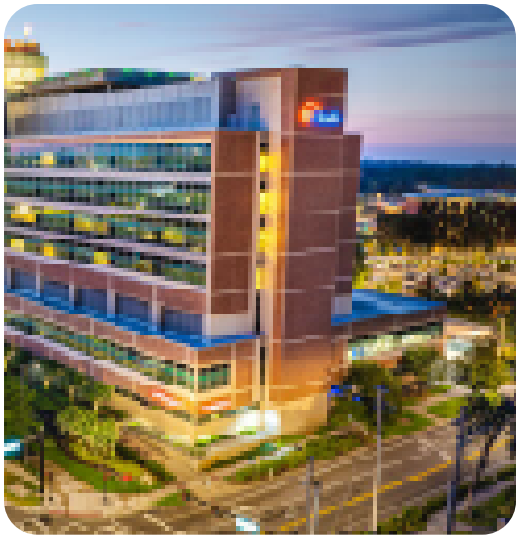
The printed records contained highly confidential data, including patient names, addresses, dates of birth, Social Security numbers, and insurance details.

Because printing was not sufficiently controlled or traceable, the employee was able to remove these printed records from the hospital environment without immediate detection.
The breach only came to light after significant damage had already occurred. This case is frequently cited in healthcare cybersecurity discussions as a clear example of how unmonitored

Incident 2:
Florida Hospital
(USA)

In a similar case involving Florida Hospital, two employees were found to have copied and printed records for approximately 9,000 patients from the eight Florida Hospital locations in Orange, Seminole and Osceola counties.
A hospital spokesperson said officials believe the incident took place from January 2012 through May 2014. The employees had legitimate access to hospital systems, which allowed them to extract information through printing without triggering immediate alerts. The printed documents were then taken outside controlled systems, exposing the hospital to regulatory scrutiny, legal action, and data breach lawsuits.

Incident 3:
UF & Shands Health Center
(Florida, USA)



At UF & Shands Health Center in Florida, a real insider breach occurred when a hospital employee used a personal mobile phone to take photos of computer screens displaying patient information, including names, dates of birth, insurance details, and Social Security numbers. The images were captured directly from hospital systems during normal work hours and were later shared with others. The incident was uncovered during a criminal investigation, leading to arrests and highlighting how photographing live hospital screens can bypass technical controls and result in serious misuse of patient data.

Similarities Across Incidents

Despite occurring in different hospitals, countries, and years, these incidents share several common characteristics:

- Insider involvement:
In all cases, the individuals involved were legitimate staff members with authorized system access.

- Use of non-technical extraction methods:
The data was leaked through printing or mobile photographing, not through hacking or malware.

- High impact on patient privacy:
Each incident involved exposure of sensitive patient information, leading to reputational, legal, and regulatory consequences.

Differences Across Incidents

Method of Data Exfiltration

- Montefiore Medical Center: Data was exfiltrated through high-volume printing of patient records, which were physically removed from the hospital.
- Florida Hospital: Data was extracted via copying and printing across multiple hospital locations.
- UF & Shands Health Center: Data was captured by taking photos of live computer screens using a personal mobile phone.

Security Control Failure

- Montefiore: Failure of print monitoring, watermarking, and auditing.
- Florida Hospital: Weak access governance and print controls across multiple sites.
- UF & Shands: Lack of screen capture prevention, Digital watermarking, and user awareness.

Recurring Vulnerabilities

Across all incidents, the following vulnerabilities repeatedly appear:

- **Anonymous printing:**
  Printed documents lacked clear attribution to a specific user or device.
- **Unprotected screens:**
  On screen data could be photographed or captured without leaving embedded evidence.

Recommendations & Preventive Measures

To effectively mitigate recurring risks, healthcare organizations must go beyond access management and introduce deterrence and accountability controls

Use of Print Watermarking

- Automatically embed user identity, device name, and timestamp on all printed pages
- Prevent anonymous printing of patient records by logging every print job.

Apply Digital Screen Watermarking

- Display persistent, visible user identification on live screens
- Ensure screenshots, photos, and recordings contain attribution

Monitor & log unauthorized Users Activities

- Correlate watermarked evidence with audit logs.
- Reduce investigation time and uncertainty when such severity incidents occur.

Targeted Training

- Provide targeted training for employees to raise awareness and prevent future data leakage incidents.

Restrict Screen Captures

- Implement screen capture controls to prevent unauthorized photographing or recording of sensitive information.

Conclusion

The incidents demonstrate that insider threats in healthcare rarely rely on sophisticated attacks. Instead, they exploit everyday actions such as printing or viewing & capturing sensitive information on a screen.

The issue was not access control, but the lack of accountability after access,

By deploying DataPatrol's Digital Watermark and using Screen Capture Prevention & Logging and Print Watermark, healthcare organizations can proactively deter insider misuse, safeguard patient privacy, without disrupting the delivery of care.

Meet healthcare compliance requirements while protecting patient trust.

www.datapatrol.com

DATAPATROL