VARONIS

2021 DATA RISK REPORT

HEALTHCARE, PHARMACEUTICAL & BIOTECH

The average healthcare worker has access to **31,000 sensitive files** on their first day of work.

CONTENTS

VARONIS

ABOUT THE REPORT

The 2021 Healthcare Data Risk Report is the second report in our annual series analyzing industry-specific threats, trends, and solutions.

This report focuses on data security in the healthcare industry: hospitals, pharmaceutical firms, and biotechnology companies. It was compiled by analyzing over 3 billion files across 58 organizations.

Many of our findings are further broken down by company size:

- **Small:** <500 employees
- **Medium:** 501–1,500 employees
- **Large:** 1,501+ employees

This report aims to help healthcare and biotech organizations better understand their cybersecurity vulnerabilities in the face of increasing threats and provides insight into how healthcare companies can mitigate future risk.

Compiled using data analysis of **3 billion files** across **58 healthcare organizations**

Hospitals

Pharmaceutical

Biotech

KEY FINDINGS

COVID-19 provided fertile ground for attackers to sow confusion and take advantage of healthcare organizations on the front lines. From hospitals triaging patients around the clock to pharmaceutical companies developing advanced vaccines, cybercriminal groups targeted entities and systems under massive stress.

Attacks against the healthcare and biotech sector demonstrate maliciousness on an unprecedented scale. While their methods vary, their goal is the same: grab sensitive data to steal, sell, or extort.

In 2020, cybercriminals unleashed potent variants of ransomware like Maze and Ryuk on hundreds of hospitals. State-sponsored actors zeroed in on pharma and biotech companies to harvest COVID-19 research. Insider threats continued to tax the healthcare sector, while simple human errors left vulnerable information exposed — posing additional risk in a year like no other. 2020 also marked the first year that a patient's death has been directly linked to a cyberattack.

With so much on the line, we wanted to understand the extent to which the healthcare and biotech sectors are protecting their sensitive information. These sectors have their work cut out for them: we found that **every employee can access one out of every five files.**[1]

Overexposed data, in tandem with an increased number of attacks exhibiting new levels of sophistication, **made healthcare one of the most at-risk sectors in 2021.**

[1] For this report, "everyone" refers to every employee within the organization.

Healthcare
Key Findings

Nearly 20% of files are open to every employee in healthcare organizations (on average)

31,000 sensitive files (HIPAA + financial + proprietary research) are **open to everyone**

Over **50% of organizations** have more than **1,000 sensitive files** open to **every employee**

About **two-thirds of organizations** have **500+ accounts with passwords that never expire**

GLOBAL FINDINGS

As Industry Threats Increase, Healthcare is Underprepared

Exposure by organization size

Organization size	Avg. # of files	Avg. # of files open to everyone	Avg. % of files open to everyone
Large	62,470,271	10,872,986	16%
Medium	49,177,666	12,767,695	23%
Small	16,686,926	4,617,693	25%
Average	**54,270,776**	**11,160,270**	**19%**

Organization size	Avg. # of folders	Avg. # of folders open to everyone	Avg. % of folders open to everyone
Large	4,742,019	887,009	16%
Medium	3,259,977	820,933	23%
Small	608,652	178,044	25%
Average	**3,894,805**	**813,052**	**19%**

Organization size	Avg. # of sensitive files	Avg. # of sensitive files open to everyone	Avg. % of sensitive files open to everyone
Large	473,215	34,435	11%
Medium	220,034	20,970	14%
Small	132,763	57,930	22%
Average	**353,701**	**30,948**	**12%**

On average, every employee has access to over 11 million files — nearly 20% of the organization's total files. But in mid- and small-sized companies, **employees have unfettered access to almost one out of every four files.**

Organization-wide exposure of personal health information (PHI) and intellectual property represents an existential risk. **On average, more than 1 in 10 sensitive files are open to every employee.**

Compared to financial services companies, the average healthcare and biotech organization has about 75% less data. While healthcare entities have fewer files, they have **a greater number of files open to every employee.** Attackers that successfully compromise one authorized device could land and expand throughout the organization or encrypt massive amounts of data with ransomware.

GLOBAL FINDINGS

State of Data Per Terabyte: Healthcare

Organization size	Files	Folders	Exposed folders	Exposed files	Uniquely permissioned folders	Exposed sensitive files	Stale, sensitive files	Unresolved SIDs[2]	Folders with inconsistent permissions	Number of reports analyzed	TB analyzed per company
Large	1,550,171	157,569	33,457	13,108	12,587	993	8,136	999	1,497	32	52
Medium	1,716,089	178,935	28,091	19,611	11,330	1,966	13,114	1,348	1,003	22	45
Small	919,923	51,774	10,888	11,888	10,474	5,107	6,425	502	851	4	56
Average	1,569,640	158,377	29,865	15,490	11,965	1,646	9,906	1,097	1,265	58	50

The average terabyte contains 1.3 million files. Approximately 2% of those (20,000 files) contain sensitive information, including patient data, proprietary research, and PII. Assessing risk per terabyte provides a clearer picture of the typical attack surface by organization size and reveals which ones are most vulnerable to insider and outsider threats.

We discovered that smaller organizations have a shocking amount of exposed data, including sensitive files, intellectual property and patient records. On their first day, new employees at small companies have **instant access to over 11,000 exposed files, and nearly half of them contain sensitive data.** This creates a massive attack surface and increases the risk of non-compliance in the event of a data breach.

Larger organizations tended to have the most problems in their permissions structures, increasing the risk of data breaches stemming from cyberattacks.

[2] Unresolved Security Identifiers (SIDs) occur when an account on an access control list is deleted from AD. Unresolved SIDs add complexity and may be exploited.

GLOBAL FINDINGS

Protecting Healthcare Data

Companies with sensitive files open to all employees via global access

Sensitive files open to everyone	% of companies
< 1,000	45%
1,000-10,000	22%
>10,000	33%

Stale sensitive data by healthcare sector company size

Company Size	Avg. # of stale sensitive files	Avg. % of sensitive files that are stale
Large	258,288	67%
Medium	146,609	67%
Small	70,980	72%
Industry average	**245,826**	**69%**

Global access groups (e.g., Everyone, Domain Users, Authenticated Users) make it possible for users within an organization to share information. When data is overexposed and underprotected, organizations can quickly lose control as employees copy, share, delete or change even the most sensitive information. Unprotected information is an easy target for cybercriminals who only need to compromise one end user to gain a foothold into your environment.

Healthcare providers and researchers must vigorously defend information protected under various regulations, including the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the GDPR in the EU. Organizations that willfully neglect HIPAA Rules and make no effort to protect sensitive patient data could be **fined up to $1.5 million per year.** Companies that fail to comply with the GDPR can be fined up to **€20 million, or 4% of annual revenue.**

More than half of hospitals, pharmaceutical companies, and biotech firms have over 1,000 sensitive files exposed to every employee. **One-third of the organizations we evaluated have over 10,000 files open to every employee.** Enforcing least privilege is a basic step every organization can take to protect data from theft and misuse while ensuring compliance with regulations.

GLOBAL FINDINGS

Authorized Personnel Only: Vulnerabilities in Active Directory

Companies with passwords that don’t expire

Passwords that don’t expire	% of companies
< 500	23%
500-1,500	36%
> 1,500	41%

Companies with ghost users

Size of stale user account group	% of companies
< 1,000	21%
1,000-10,000	57%
> 10,000	22%

“Ghost users” — user and service accounts that are inactive but still enabled — give hackers an easy way to move through an organizations’ file structures undetected. Hackers often exploit this weakness to steal data or disrupt critical systems.

Varonis data analysis reveals that the healthcare sector falls well below average when finding and fixing this vulnerability. **77% of the companies we surveyed have 501 or more accounts with passwords that never expire, while 79% have more than 1,000 ghost users still enabled.**

STATE OF THE INDUSTRY

If 2020 portends what the future holds, cyberattacks targeting the healthcare sector will only worsen.

While medical professionals made COVID-19 vaccination breakthroughs at an astounding rate, confirmed data breaches also increased by a staggering 58% as bad actors targeted vaccine research and high-priority intellectual property.

The industry was woefully underprepared for these attacks. A mere 23% of healthcare organizations have fully deployed security automation. The result of this is an average breach lifecycle of 329 days — the highest of any industry — and an average **data breach cost of $7.13** million in 2020 — a 10.5% increase over 2019.

Cyberattacks were also more sophisticated than anything in years prior. Examples include a global intrusion campaign that trojanized SolarWinds Orion business software updates to distribute a new type of malware called SUNBURST. This attack still has wide-ranging consequences and continues to affect government, consulting, technology, telecom entities.

To get in front of increasingly malicious and sophisticated cyberattacks, hospitals, pharmaceutical companies, and biotechs need to double down on maturing incident response procedures and mitigation efforts. Enforcing least privilege, locking down sensitive data, and restricting lateral movement in their environments are the absolute bare minimum precautionary measures that healthcare organizations need to take.

The average cost of a data breach in the healthcare sector was **$7.13 million in 2020.**

CASE STUDY

How Varonis helps a Top-20 Operator of Urgent Care Clinics resolve security incidents quickly and conclusively

When an insider accessed 15,000 files in quick succession, Chris had mere minutes to figure out if his company was under attack and kill the threat before it resulted in a data breach.

Find out how Varonis helps.

DOWNLOAD THE FULL CASE STUDY

VARONIS

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, specializing in software for data protection, threat detection and response, and compliance. Varonis protects enterprise data by analyzing data activity, perimeter telemetry, and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

> *To go through our main file server and lock it down the way Varonis does — it would be a multi-year project, requiring my entire team, and we probably still wouldn't be done."*

CHRIS M.
System Engineer

Want to see how **your organization** stacks up?

Get a free Varonis Data Risk Assessment. Uncover hidden risks to your most important data — fast, and without adding work to your plate.

CONTACT US

Trusted by

BlueCross BlueShield

Seattle Cancer Care Alliance

Hugh Chatham Memorial Hospital

AHIP America's Health Insurance Plans

CENTRE HOSPITALIER THÉOPHILE ROUSSEL

Centre Hospitalier Alpes-Isère

CENTRE HOSPITALIER Princesse Grace

Mercy Health Care first

La Renaissance Sanitaire

Fresenius Netcare

LEXINGTON MEDICAL CENTER

Louis Pasteur Santé LORRAINE

Children's Hospital and Health System

CAPE COD HEALTHCARE

imelda ZIEKENHUIS

Cerba HealthCare

Centre Hospitalier Sud Francilien

GROUPE HOSPITALIER PAUL GUIRAUD

LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE

VARONIS

www.varonis.com