BLOG– Network Folders: Access, Privacy & Stale Data—Oh My!

Posted by: William | On: April 2, 2026 | Data Privacy, Guides & Best Practices

https://wardtechaudit.com/network-folders-access-permissions-privacy-and-stale-data-oh-my/

Network Folders: Access, Privacy & Stale Data—Oh My!

Why you should know ***What*** *data is stored on your network,* ***Who*** *has access, &* ***What*** *to do about it.*

Summary Table of Contents

Introduction

"Security through obscurity" — Sounds clever—but in practice, it's a dangerous assumption.
If your organization doesn't clearly understand what data exists on its network shares and who can access it, you're not secure—you're exposed.

Across industries, network folders quietly accumulate years of sensitive, redundant, and poorly controlled data. And when something goes wrong—an audit, a breach, or an internal incident—this hidden risk surfaces fast.

What's Stored in Your Network Folders (And Why It's Risky)

Most organizations underestimate what's sitting in their shared drives. In reality, **network folders often contain**:

- **Sensitive personal data** – PII and PHI such as Social Security numbers, health records, and financial details
- **HR-related data** – Salary information, performance reviews, disciplinary records, and employee grievances
- **Confidential company information** – Financials, forecasts, strategic plans, and intellectual property
- **Unstructured personal content** – Files employees saved "temporarily" but never removed
- **Stale or redundant data** – Old backups, test data, duplicate files, and former employee folders

Over time, these folders become a mix of **high-risk data and low-value clutter**—with little visibility or control.

Why This Matters More Than You Think

1. Data Privacy & Compliance Risk – Regulations like GDPR, CCPA, and HIPAA require strict control over sensitive data. If it's sitting in open or poorly controlled folders, you may already be out of compliance—without realizing it.

2. Financial Risk – Exposure of salary data, financials, or proprietary information can lead to fraud, legal costs, and regulatory penalties.

3. Reputation Risk – Internal data leaks can be just as damaging as external breaches. Employees or contractors gaining access to inappropriate data can quickly erode trust.

4. Operational & Cost Impact – Stale and duplicate data increases:

- Storage costs
- Backup and recovery time
- Complexity in audits and investigations

Many organizations are paying significantly more than they should—just to store data they don't need.

What We See in Real Audits

Here's the uncomfortable truth: **We've never encountered an organization that had network folders fully locked down. In audit after audit, we've found:**

- Gigabytes (or even terabytes!) of **unsecured sensitive data**
- Open access to folders **containing HR, financial, and legal information**

- Years of **unreviewed, duplicated, and outdated files**

Examples include:

- Employee health records and salary data
- HR investigations and grievance files
- Social Security numbers stored in spreadsheets with names and contact information
- Personal employee data (including highly sensitive personal situations)
- Confidential executive and company information

This is not the exception—**it's the norm.**

How to Start Cleaning It Up and Secure Your Network Folders

1. Use Automated / Specialized Tools

Start with tools that can:

- Scan for, and identify, **sensitive data (PII/PHI)**
- Map **user access and permissions**
- Detect **stale, duplicate, or orphaned data**

Examples:

- Microsoft Purview
- Varonis
- Netwrix

2. Take a Structured DIY Approach to Access Reviews & Cleanup

If automated, specialized tools aren't immediately available, use Active Directory and command-line commands or scripts, and start with:

- **Access/Permissions reviews** – Identify folders with broad access (e.g., "Everyone") and secure them to least privilege access as needed
- **Data classification** – Tag or categorize sensitive vs non-sensitive data
- **Cleanup efforts** – Remove duplicates, archive appropriately, and delete what's no longer needed
- **Ownership assignment** – Ensure every folder has a responsible owner

💡 **Important Tip: Secure the Cleanup Process**

Ironically, cleanup efforts can create new risks.

- Limit the cleanup effort access to **trusted individuals only**
- Log & review/approve all activity during discovery and remediation
- Avoid copying sensitive data into less secure locations during analysis

Why This Isn't a One-Time Fix

Even if you clean everything up today, the problem will come back.

Why?

- New employees create folders
- Data gets copied for convenience
- Systems and processes change
- Mistakes happen

Ongoing best practices:

- Schedule **regular access reviews**
- Monitor for **sensitive data in shared locations**
- Enforce **least privilege access**
- Periodically review **stale and orphaned data**

Real-World Example of a Data Exposure Risk

*"**Bob**" from HR is preparing for the new year.*

He copies all files from a secure HR folder into a new "Archive" folder he created—thinking it's restricted to HR only. The files include salary and bonus information used by leadership.

After copying, he deletes the original secure files.

*What Bob doesn't realize: His new "Archive" folder is in a location where **Everyone** in Active Directory has access.*

No one notices.

Each year, Bob repeats the process—adding more sensitive data to the same folder.

One, two (or five) years later, someone stumbles across it… and shares it.

👉 This scenario occurs **far** more often than organizations expect or know.

From Hidden Risk to Controlled Environment

Network folders are often overlooked—but they represent one of the **largest unmanaged risk areas** in most organizations.

The goal isn't perfection—it's visibility and control:

- Know what data you have
- Know who can access it
- Remove what you don't need
- Continuously monitor what changes

Final Thoughts: Don't Rely on Assumptions

If you haven't reviewed your network folders recently, **assume there are gaps.**
Because in practice—***there always are*.**