



DLP Suite for Healthcare



Your Patient PHI is Leaking Right Now. Identity Finder will Stop it.

Even HIPAA-compliant hospitals and healthcare organizations leak Protected Health Information (PHI) and Electronic Health Records (EHR) on a daily basis. Physicians send EHRs to hospitals but save copies on computers and in emails. Authorized employees unwittingly copy data containing PHI from core health information systems in order to perform their jobs. These leaked copies of PHI sit like landmines on your workstations and servers waiting to become a breach. Identity Finder discovers potential PHI leaks and secures unprotected PHI before it leads to a breach.

How Information Leakage Occurs

Even if your core Health Information System (HIS) is HIPAA-compliant and guarded by a small army of IT security professionals, sensitive PHI leaks to places it shouldn't be. Consider these common examples:

- **File Servers:** A dictation service transmits typed notes to a physical therapist who saves a copy on a local file server before copying the information to the HIS.
- **Laptops:** A billing department employee calls a patient, who pays with a credit card. The employee types the credit card number into an Excel Spreadsheet on his laptop before issuing the charge.
- **E-mail Servers:** A patient emails a physician his social security number and symptoms, who enters the information into the HIS, but forgets to delete the email.
- **Backups:** The IT department makes regular backups of critical health information systems, which are stored in various locations.
- **Databases:** The radiology department maintains a smaller copy of the hospital system's HIS with specialized radiology PHI.
- **USB and Flash Drives:** A local InstaCare employee saves PHI to a thumb drive so she can work from home prior to entering the report into the HIS.

How Identity Finder DLP for Healthcare Helps You

Identity Finder DLP searches devices ranging from a laptop to large networks of servers to find and secure errant PHI stored on hard drives. Identity Finder's AnyFind™ technology automatically identifies true Social Security Numbers, medical record numbers, and other confidential patient data.

→ Search Data-at-Rest

- Windows/Mac Desktops/Servers
- NAS, Linux, and UNIX Devices
- SQL, Oracle, and Databases
- E-Mail Applications and Servers
- Websites and SharePoint

→ Discover PHI/EHRS

- Social Security Numbers
- ICD 9, ICD 10, and CPT Codes
- Drivers Licenses
- Dates of Birth and Addresses
- Credit Cards and Bank Accounts

→ Protect and Secure

- Comply with HIPAA and HITECH
- Shred, Redact, and Encrypt
- Quarantine

→ Report

- Centralized Reporting
- Technical Level Reports
- Trending Analysis
- Gap Analysis

DLP Suite for Healthcare



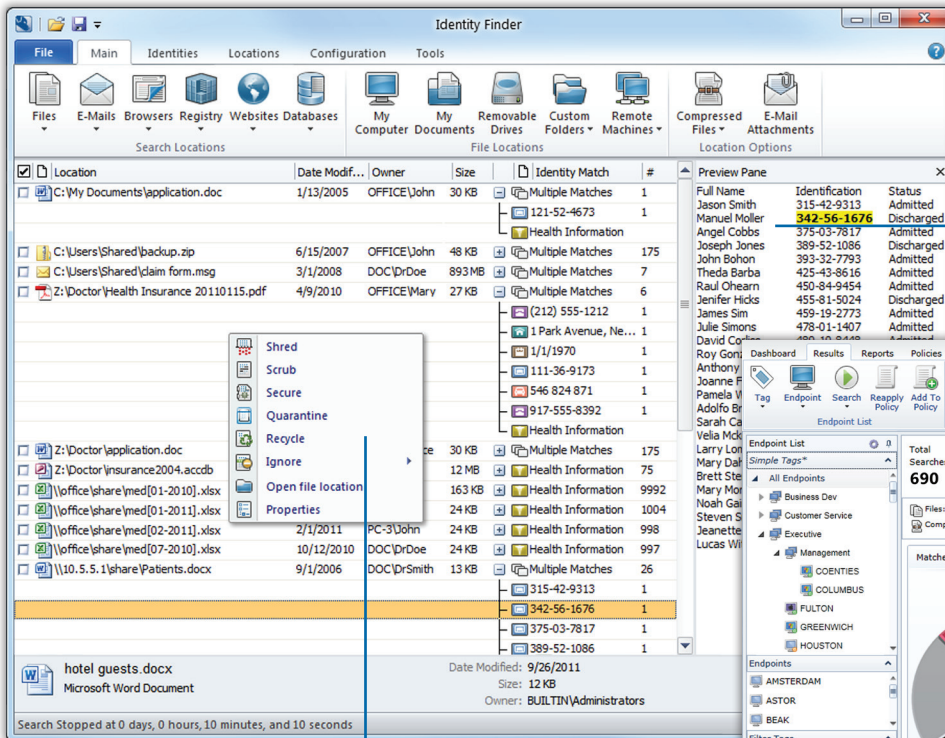
DLP Endpoint for Windows and Mac | DLP Console

Identity Finder DLP Endpoint prevents data loss in hospital systems by finding and securing errant PHI and EHRs. The AnyFind™ engine accurately discovers sensitive information stored on desktops, servers, remote computers, databases, websites, and removable drives. The DLP Console provides centralized control and reporting.

Requirements:

DLP Endpoint: Windows (x86 or x64) version 7, Vista, XP, Server 2003 or higher; Mac OS X (Intel) 10.5 or higher.

DLP Console: Windows Server 2008 or higher with IIS. SQL Server 2008 or higher.



The DLP Endpoint interface is easy to use by administrators and end users. Find and protect sensitive information across your hospital's environment.

The DLP Endpoint's remediation features allow end users to Shred, Redact, Encrypt, and Quarantine unprotected data.

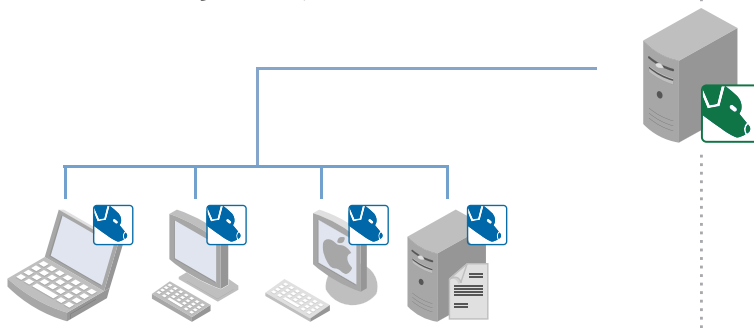
The DLP Console's dashboard provides access to executive level and technical reports.



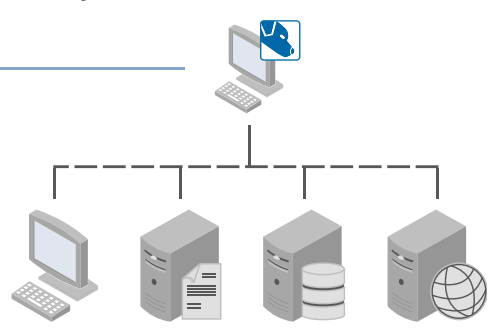
Identity Finder DLP Enterprise Architecture

Legend: DLP Endpoint DLP Console

Managed Endpoints



Agentless Search



About Identity Finder

Identity Finder, LLC was founded in 2001 and is headquartered in New York. Its security and privacy technologies provide businesses and consumers the ability to prevent data leakage and identity theft. The company has quickly grown to become a leader in data loss protection and identity fraud prevention by helping millions of consumers, small businesses, and enterprises in over fifty countries.

Identity Finder World Headquarters

250 West 57th Street, Suite 2412
 New York, NY 10107 USA
 Toll Free: +1 888 244 3790
 Fax: +1 888 206 6389
www.identityfinder.com