proofpoint.

DSPM: Protecting PHI, research data and intellectual property starts with visibility

Healthcare and life sciences organizations are rapidly digitizing care delivery, claims processing and drug development while simultaneously deploying AI agents to accelerate operations and research. But as sensitive data spreads across cloud platforms, partner ecosystems and autonomous AI systems, security teams face growing visibility gaps and regulatory pressure.

"Healthcare and life sciences organizations are experiencing explosive growth in unstructured data from clinical records and claims data to research and AI models. Much of that data is highly sensitive and often overshared across complex ecosystems."

— Derek Maki
SVP, Head of Product for Data Security, Proofpoint

For years, healthcare providers, insurers and life sciences companies relied on perimeter defenses, data loss prevention (DLP) tools as well as security information and event management (SIEM) platforms to safeguard patient and research data. Those tools were built for a time when data stayed inside hospital networks, corporate data centers and controlled research systems.

Today, healthcare data is everywhere.

Electronic health records move between providers and payers. Claims data flows through third-party administrators. Clinical trial data is shared with clinical research organizations (CROs) and research partners. Pharmaceutical intellectual property lives in multi-cloud environments. AI models are trained on vast volumes of structured and unstructured data.

This digital acceleration has created a critical visibility gap.

"Healthcare and life sciences organizations are experiencing explosive growth in unstructured data from clinical records and claims data to research and AI models," said Derek Maki, SVP, head of data security product at Proofpoint. "Much of that data is highly sensitive and often overshared across complex ecosystems."

Sensitive data including protected health information (PHI), personally identifiable information (PII), genomic data, payment information and proprietary research is frequently stored across SaaS applications, cloud storage, collaboration platforms and hybrid environments. Files may be misconfigured, broadly accessible or shared externally without full awareness.

At the heart of the issue is a simple reality: You can't protect patient trust, research breakthroughs or healthcare revenue if you don't know where your sensitive data lives.

Data visibility across the healthcare ecosystem—from discovery to care delivery

To regain control, healthcare organizations are adopting data security posture management (DSPM)—a modern framework that continuously discovers sensitive data, analyzes access risk and prioritizes remediation.

"With the scale of data across providers, health plans and life sciences organizations, it's incredibly difficult to know where your most sensitive data resides," Maki explained. "DSPM gives organizations the ability to identify high-risk data stores, understand who has access and focus on the risks that matter most."

DSPM continuously scans environments to identify:

- Overshared patient records
- Misconfigured cloud storage containing PHI
- Excessive access to claims and financial systems
- Unprotected clinical research data
- Exposed intellectual property and sensitive datasets, including those used in AI training

Rather than flooding teams with alerts, DSPM provides context—combining data sensitivity, access exposure and threat paths to prioritize real risk.

For security teams managing compliance obligations such as HIPAA, HITRUST, PCI DSS, FDA requirements and global data protection regulations, this visibility is transformative.

"Providers, payers and pharmaceutical companies all face the same challenge: massive data sprawl and limited security resources," said Maki. "Risk prioritization is essential to protect patient data, research and revenue."

"Providers, payers and pharmaceutical companies all face the same challenge: massive data sprawl and limited security resources. Risk prioritization is essential to protect patient data, research and revenue."

— Derek Maki
SVP, Head of Product for Data Security, Proofpoint

Securing the rise of AI agents in healthcare and life sciences

Across the healthcare ecosystem, AI agents are being embedded into clinical workflows, claims processing, drug discovery and patient engagement platforms. These agents access vast amounts of PHI, research data, financial records and proprietary intellectual property—often across multiple cloud environments.But unlike traditional users, AI agents:

- Operate autonomously
- Access data dynamically
- Interact with multiple systems simultaneously
- Create new, complex data flows
- Introduce non-human identities into access models

This creates a new layer of risk that many healthcare organizations struggle to track.

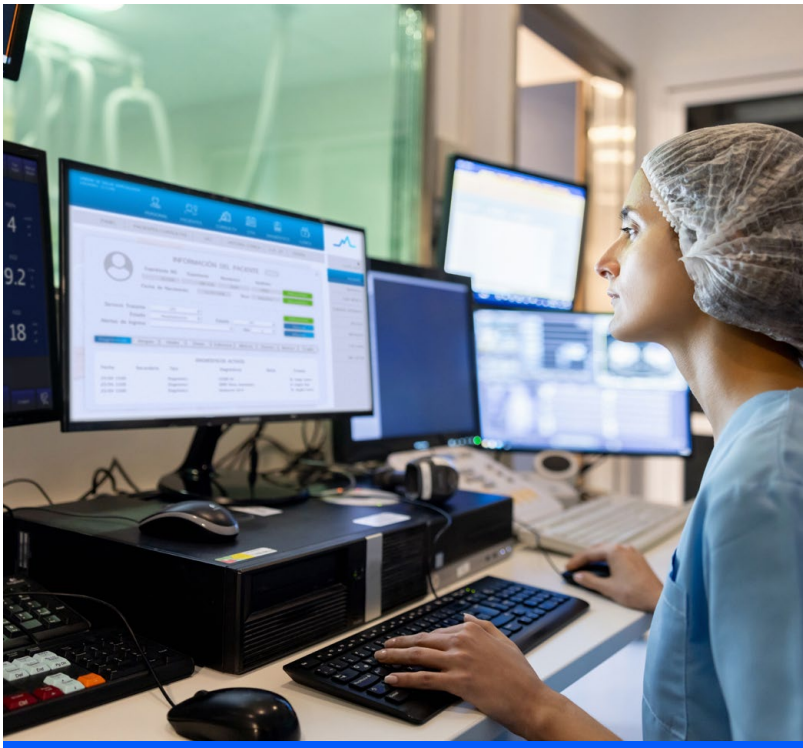
"Healthcare organizations are rapidly deploying AI agents to drive efficiency and innovation," Maki explains. "But those agents require broad access to sensitive data. Without clear visibility into what they're accessing, where that data flows and how permissions evolve, organizations introduce significant and often unseen risk."

AI models trained on clinical records, claims data or genomic research can inadvertently expose regulated information. Over-permissioned AI service accounts can create indirect attack paths to patient data or proprietary drug research.

By mapping identities—including non-human identities and service accounts—alongside data sensitivity and access exposure, Proofpoint DSPM helps healthcare organizations:

- Identify where AI agents have excessive permissions
- Understand which sensitive datasets are being used to train or power AI
- Detect oversharing and misconfigured AI service accounts
- Visualize indirect access paths created by automation
- Reduce the risk of AI-driven data exposure

"In the era of AI-driven healthcare, visibility into non-human access is just as important as visibility into human access," Maki added. "DSPM gives organizations the context they need to innovate confidently while protecting patient trust and intellectual property."



"In the era of AI-driven healthcare, visibility into non-human access is just as important as visibility into human access. DSPM gives organizations the context they need to innovate confidently while protecting patient trust and intellectual property."

— Derek Maki
SVP, Head of Product for Data Security, Proofpoint

Inside Proofpoint's DSPM: intelligent protection for healthcare and life sciences

Proofpoint's DSPM is purpose-built for highly regulated industries with complex ecosystems like healthcare. Rather than adding more operational burden, it delivers rapid visibility and measurable risk reduction.

- **Rapid, agentless deployment**
  Proofpoint connects via API to Microsoft 365, Google Workspace, AWS and other cloud platforms — with no agents and minimal disruption. Healthcare organizations can begin discovering and classifying sensitive data quickly across clinical, corporate and research environments.

- **Comprehensive, scalable discovery**
  Proofpoint's One-Pass Scanner identifies and classifies PHI, PII, payment data, proprietary research, clinical trial data and other sensitive information across SaaS, PaaS, IaaS, on-premises and hybrid environments — while maintaining data residency requirements.

- **AI agent and non-human identity visibility**
  Proofpoint maps and analyzes non-human identities — including AI agents, service accounts and automation workflows — to identify excessive permissions, sensitive data exposure and indirect access paths created by machine-driven processes.

- **Attack path and access risk visualization**
  Access and attack path mapping reveals how identities, permissions and data stores intersect — exposing indirect access routes to patient records, claims systems or research repositories.

- **Automated remediation and enforcement**
  Proofpoint provides one-click DLP policy creation to revoke excessive permissions through Proofpoint DLP and integrates with tools like ServiceNow, Jira and Slack for guided remediation workflows.

A smarter way to protect patient data, research and innovation

Healthcare and life sciences organizations must balance innovation with strict regulatory compliance and patient trust.

"Without accurate data classification, you can't enforce HIPAA safeguards, protect clinical research or secure proprietary drug development data," Maki said. "Proofpoint automates classification so healthcare organizations can apply the right controls without slowing innovation."

In an industry where a single data breach can disrupt care delivery, delay research or erode patient trust, clarity and control are no longer optional.

Proofpoint DSPM delivers the visibility, prioritization and automation healthcare organizations need to protect what matters most.

Proofpoint DSPM helps organizations:

- Identify and protect PHI across distributed systems
- Safeguard proprietary drug research and clinical data
- Govern AI agent access to sensitive datasets and reduce non-human identity risk
- Reduce breach likelihood and financial exposure
- Align with HIPAA, HITRUST and global compliance requirements
- Quantify risk with data value and breach likelihood insights

"Without accurate data classification, you can't enforce HIPAA safeguards, protect clinical research or secure proprietary drug development data. Proofpoint automates classification so healthcare organizations can apply the right controls without slowing innovation."

— Derek Maki
SVP, Head of Product for Data Security, Proofpoint

Learn how

Proofpoint helps healthcare and life sciences organizations discover, classify, and govern sensitive data at scale.