proofpoint

SOLUTION BRIEF

Secure Healthcare AI Adoption at Scale

Governing data, identity, and agentic risk across clinical and operational AI workflows



Healthcare organizations are rapidly moving from AI experimentation to AI-enabled operations. What began with focused use cases such as clinical documentation, coding support, contact center assistance, and revenue cycle optimization is quickly expanding into workflows that connect clinicians, patients, payers, data platforms, and third-party applications.

Key Highlights

- Discovers sanctioned and shadow AI usage across clinical and administrative teams
- Classifies and monitors sensitive healthcare data—PHI, PII, PCI/cardholder, claims, and pharmacy data—that AI tools can access
- Blocks sensitive files and content from being uploaded to unsanctioned AI applications
- Inspects and blocks prompts containing regulated data before they reach sanctioned AI services
- Applies real-time guardrails to detect and remediate risky AI interactions
- Governs AI agents and non-human identities acting across healthcare systems

© Proofpoint, Inc 2026

As AI becomes embedded across clinical and operational workflows, healthcare organizations need more than an approved application list. They need governance that controls how people, AI agents, and the sensitive data they access interact across the continuum of care.

Proofpoint Data and AI Security provides a governance and control layer around AI use, reducing the risk of sensitive data exposure, over-permissioned access, shadow AI, prompt and output leakage, and agent misuse so healthcare organizations can innovate with confidence.

The New Healthcare AI Risk Surface

Traditional security programs assume people access applications and data in predictable ways. AI changes that model. Sensitive information now flows through prompts, uploads, summaries, agent memory, and autonomous actions, while AI assistants and agents can access multiple systems on behalf of users.

As a result, healthcare organizations need to govern more than applications alone. They need visibility into how AI interacts with sensitive data, identities, and business systems across every workflow.

This creates five new categories of risk:

1. **Sensitive data exposure—**PHI, claims, and behavioral health data pasted into AI prompts, uploads, or copied out of AI-generated responses
2. **Shadow AI—**unsanctioned or departmentally procured tools used outside central governance, with unknown data retention or training practices
3. **Agentic risk—**AI agents that plan tasks, call APIs, and act across systems, introducing a new class of non-human identity to govern
4. **Over-permissioned access—**AI tools and agents that inherit overly broad access to SharePoint, mailboxes, and data stores
5. **Lack of auditability—**no reliable way to reconstruct what data an AI interaction touched or what action an agent took

The Solution: Proofpoint Data and AI Security

Healthcare organizations don't just need to secure AI applications. They need to secure how people and AI work together every day. Employees continue to make decisions and handle sensitive information, while AI assistants and agents increasingly access the same data, systems, and workflows.

Proofpoint extends existing data security controls to AI by combining visibility, data protection, and runtime governance in a single control plane. It sits between healthcare users, AI agents, and the clinical and administrative systems they access, helping organizations govern AI interactions without disrupting existing workflows.

Rather than securing only the AI application, Proofpoint applies controls across every AI interaction—from discovering AI use to governing prompts, sensitive data, and agent behavior. The image below shows the five control layers that secure healthcare AI adoption. In the sections that follow, we'll explain how each layer reduces AI risk.

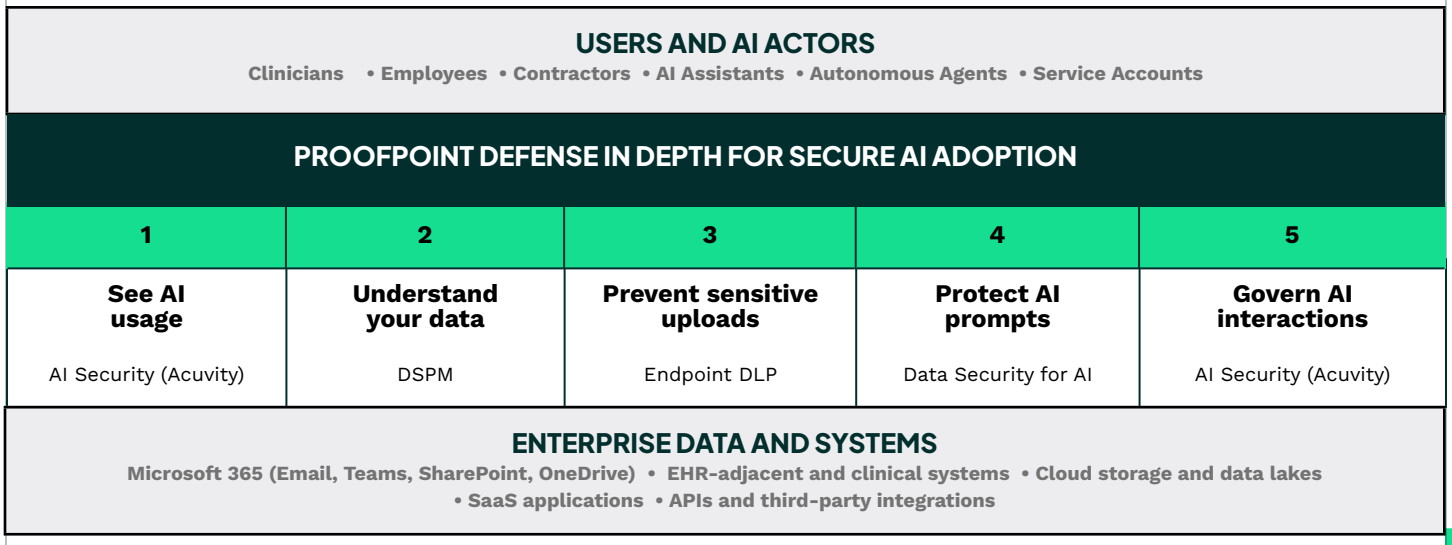


Figure 1. The Proofpoint Data and AI Security control plane sits between healthcare users and AI agents and the enterprise systems that they touch.

© Proofpoint, Inc 2026

The five layers work together to address each stage of AI interaction—from discovering AI usage to governing AI behavior.

1. **See AI usage.** Proofpoint AI Security helps healthcare organizations discover every sanctioned and shadow AI application in use across the organization, including embedded AI features in SaaS platforms. As a result, security teams know where risk exists before it becomes an incident.
2. **Understand your data.** Proofpoint Data Security and Posture Management (DSPM) classifies and monitors sensitive healthcare data across health IT sources to understand what AI tools and agents can access, and where exposure or over-permissioned access already exists.
3. **Prevent sensitive uploads.** Proofpoint endpoint DLP blocks regulated files and content—PHI, PII, PCI, claims, and pharmacy data—from being uploaded or shared with any AI application (sanctioned or not) at the endpoint. It does this using the same endpoint sensor that currently protects against sensitive data from being inappropriately printed or being transferred to removable storage.
4. **Protect AI prompts.** Proofpoint Data Security for AI inspects prompts sent to sanctioned AI services and blocks or redacts sensitive information before it reaches the model. This closes the most common path for accidental data loss.
5. **Govern AI interactions.** Proofpoint AI Security applies real-time guardrails across sanctioned apps to detect and remediate prompt injection, jailbreaking, unsafe tool use, data exfiltration, and policy violations.

Governance outcomes

- PHI protection
- Reduced shadow AI risk
- Least-privilege access
- Agent accountability
- Improved auditability
- Safer AI adoption

Protecting Sensitive Healthcare Data in AI Workflows

Beyond broad categories such as PHI and PII, healthcare organizations need visibility into the specific data signals that appear throughout AI workflows. Proofpoint identifies these signals and applies the appropriate controls based on how and where the data is used.

© Proofpoint, Inc 2026

The table below shows common healthcare data signals, the risks they introduce, and the Proofpoint controls that help govern them. These controls become even more valuable when applied across the AI workflows that healthcare organizations rely on every day.

Sensitive data signal	Example healthcare risk	Proofpoint control
SSNs and other PII	Exposed in email attachments, uploads, or AI prompts	Email DLP + Endpoint DLP + DS for AI
PCI / cardholder data	Payment or billing details entered into AI tools or shared files	DSPM + Endpoint DLP
ICD-10 and clinical codes	Diagnosis codes surfaced in AI outputs, creating HIPAA exposure	Endpoint DLP + DSPM + DS for AI
Copy to removable media	PHI copied to USB or external drives	Endpoint DLP
Print activity	Clinical or billing records printed outside policy	Endpoint DLP
Web and AI uploads	PHI uploaded to unsanctioned AI tools or websites	Endpoint DLP + DS for AI

Operational impact

The following examples illustrate how Proofpoint helps govern AI across common clinical and administrative healthcare workflows.

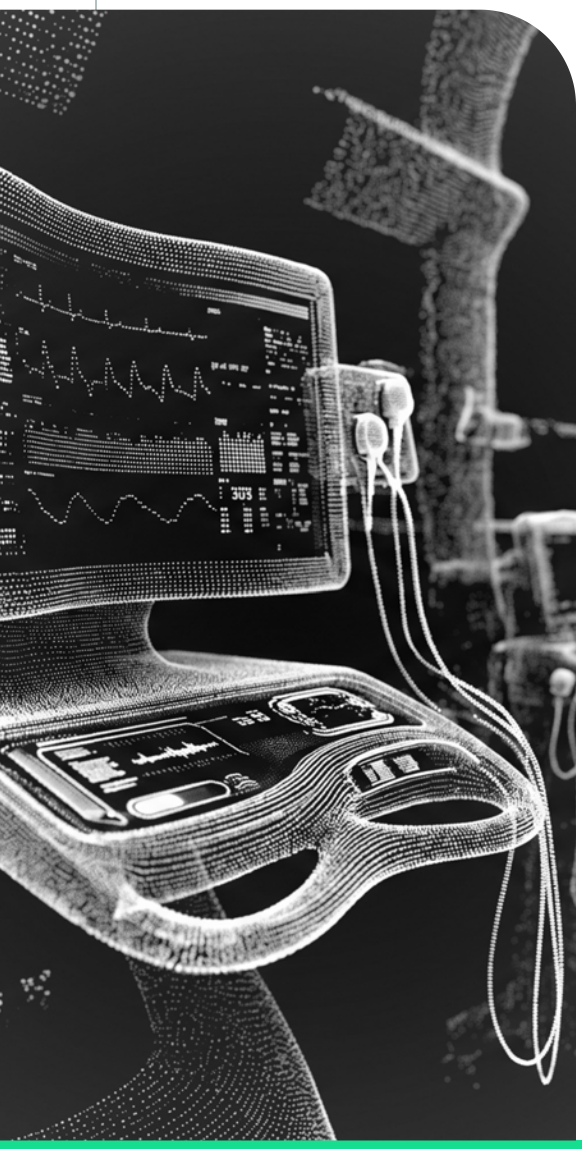
Clinical documentation and ambient AI security

Clinicians increasingly rely on ambient listening and AI documentation tools. They often use several different platforms across specialties and departments—not just one approved system—to generate encounter notes and after-visit summaries. Proofpoint governs the ecosystem around these workflows. It confirms where summaries are stored; whether outputs are copied into email, EHR-adjacent systems, or shared drives; whether coding and billing suggestions derived from ambient AI carry PHI downstream; and whether follow-on AI tools are used to repurpose clinical notes without an audit trail.

Point-of-care clinical AI (such as OpenEvidence)

Physicians are turning to point-of-care clinical AI tools like OpenEvidence to get fast, literature-backed answers during patient encounters. Because these tools accept free-text queries, clinicians can unintentionally include patient specifics. This creates risks for PHI exposure and shadow AI that sits outside IT's visibility. Proofpoint helps discover this usage across the organization, prevents identifiable patient data from being entered into prompts, and provides the audit trail needed to show how the tool was used.

© Proofpoint, Inc 2026



Prior authorization and claims automation

Payer and health plan teams use AI to summarize medical records, validate eligibility, and draft prior authorization responses—all of which are workflows that touch PHI, claims data, and member communications. Proofpoint monitors what sensitive data enters approved AI tools, flags risky shadow AI use, and provides evidence of how AI-generated content was handled.

Agentic workflows across enterprise systems

AI agents built to validate provider directories, route exceptions, or process benefit requests may touch email, attachments, and internal databases. Proofpoint helps confirm agents act within scope, aren't over-permissioned, and don't expose PHI unnecessarily with a full record for audit.

Shadow AI across administrative departments

Finance, HR, legal, and patient experience teams use AI to summarize documents and draft communications often touching sensitive patient, employee, or financial data even outside clinical workflows. Proofpoint discovers this unsanctioned use, applies data-aware policy controls, and coaches users toward safer behavior.

M365 Copilot and collaboration data

Healthcare organizations need to know what sensitive data already sits in email, Teams, SharePoint, and OneDrive and whether permissions around it are appropriate. Proofpoint helps identify sensitive data exposure and risky access patterns across collaboration environments that may become AI context.

Learn More

For more information, visit **proofpoint.com.**

proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.
© Proofpoint, Inc 2026