imprivata

DATASHEET

Aligning agentic AI governance with Health Sector Coordinating Council (HSCC) guidance

How Imprivata helps healthcare organizations secure, govern, and monitor AI agent access

Agentic AI is rapidly reshaping healthcare workflows. It has the potential to reduce administrative burdens, support and empower clinicians, and increase operational efficiency. But AI agents don't operate in a vacuum. They may interact with EHRs, PHI, clinical workflows, pharmacy systems, identity platforms, or other critical infrastructure.

As a result, they introduce a new and urgent risk. *The Health Sector Coordinating Council (HSCC) Third-Party AI Risk and Supply Chain Transparency Guide* calls for healthcare organizations to conduct additional threat modeling when AI solutions include autonomous or semi-autonomous agents, treating them as a new category of insider threat.

Imprivata recognizes the opportunity and challenges that agentic AI presents for healthcare delivery organizations, and we continue to innovate across our portfolio to support the safe, secure, and compliant implementation of autonomous AI-powered workflows. By extending identity and access controls to AI agents, organizations can see what each agent is, control what it can access, and monitor its behavior. The same security principles that govern human and third-party access now apply to non-human identities.

How Imprivata supports the HSCC recommendations

HSCC agentic AI recommendations	Healthcare risk	How Imprivata helps
Verify every AI agent has a unique identity with documented capabilities and boundaries.	"Invisible" agents can access systems without accountability, making it difficult to understand who or what acted.	Imprivata can register or auto-discover AI agents as managed identities, defines access policies, and controls what systems and actions each agent can perform.
Manage AI credentials with the same rigor as privileged service accounts.	Static credentials, shared accounts, or unmanaged secrets can expose EHRs, PHI, and privileged systems.	Imprivata brokers secure access so agents do not store or handle credentials. Access is controlled through sessions and short-lived authentication.
Establish behavioral baselines for each AI agent.	AI agents can operate continuously and at machine speed, making abnormal activity harder to identify manually.	Imprivata applies AI-based anomaly detection, peer modeling, risk scoring, and user/entity behavior analytics to support behavior-based visibility.
Monitor for rogue behavior, unexpected data access, and privilege escalation.	A compromised or drifting agent could access inappropriate records, escalate privileges, or trigger unsafe automation.	Imprivata supports real-time monitoring, suspicious behavior detection, session investigation, and immediate revocation or termination of access for unexpected AI agent activity.

HSCC agentic AI recommendations	Healthcare risk	How Imprivata helps
Scope and constrain EHR access.	HSCC warns that an AI agent with excessive EHR permissions is comparable to a compromised insider with clinical system privileges.	Imprivata enables least-privilege access across modern and legacy healthcare systems, with auditability and policy enforcement for agents accessing critical systems.
Validate AI agent permissions and behavioral monitoring before deployment.	Controls that look good on paper may fail in real clinical workflows.	HSCC calls for security validation, audit logging, authentication and authorization testing, least-privilege verification, and behavioral monitoring tests before production. Imprivata provides the identity, access, monitoring, and audit capabilities that support those validation activities.
Protect patient privacy and support investigation.	AI agent access to PHI must be explainable, auditable, and reviewable by privacy and compliance teams.	Imprivata uses AI to track PHI access, investigate risks, detect high-risk behavior, support audit trails, and monitor EHR access at scale.

AI agents are becoming a part of everyday healthcare workflows. But they have the power to cause far more damage than traditional users can. HSCC guidance makes it clear that AI agents need the same identity, access, and monitoring controls as any other user to minimize that risk.

Imprivata helps healthcare organizations extend security controls to AI agents, protecting new workflows without slowing down the people who rely on them.

Take the next step: Learn more about how Imprivata secures AI agent access to enterprise systems. Watch the on-demand webinar.

imprivata

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

6999-2026_AIM-DS-HSCC-AI-guidance