Censinet, AHA, and the Scottsdale Institute Launch the 2026 Healthcare Cybersecurity Benchmarking Study

Additional 2026 Sponsors Include Health-ISAC, HSCC, and The University of Texas at Austin; Study Helps Drive Enterprise Cyber Resilience, Stronger AI Governance

BOSTON, MA, UNITED STATES, September 9, 2025 /EINPresswire.com/ -- Censinet, the leading provider of healthcare risk management solutions, today announced that enrollment is now open for the 2026 Healthcare Cybersecurity Benchmarking Study, the industry's landmark annual initiative delivering robust, objective, and actionable benchmarks to strengthen cybersecurity across the health sector. Co-sponsored by the Scottsdale Institute, the American Hospital Association (AHA), Health Information Sharing and Analysis Center (Health-ISAC), the Healthcare and Public Health Sector Coordinating Council (HSCC), and new sponsor The University of Texas at Austin, the Benchmarking Study helps healthcare organizations prioritize cybersecurity investments by assessing and improving preparedness, advancing AI governance maturity, and increasing the maturity and efficiency of cyber programs to strengthen resilience against high-impact attacks. To enroll in the 2026 Benchmarking Study or learn more, email benchmarks@censinet.com. The 2025 Benchmarking Study summary report can be found here.

> The Scottsdale Institute is honored to support the 2026 Healthcare Cybersecurity Benchmarking Study, which is essential to strengthening the trust, safety, and resilience of our healthcare system"
>
> *Janet Guptill, President and CEO of the Scottsdale Institute*

"Since inception four years ago, the Benchmarking Study has activated a national discussion on healthcare cybersecurity and brought together over 250 healthcare organizations to help shape industry best practices," said Ed Gaudet, CEO and Founder of Censinet. "This year's study comes at a pivotal moment, as nation state-supported actors increasingly target the critical functions that sustain patient care and as AI adoption rapidly accelerates, potentially beyond our ability to effectively govern its risks. The 2026 Benchmarking Study will help healthcare leaders strengthen resilience, close AI governance gaps, and ensure innovation advances without compromising patient safety."

Exclusive Benefits for 2026 Benchmarking Study Participants

Participation in the 2026 Benchmarking Study is free of charge and gives organizations access to enterprise assessments and peer comparisons to strengthen cybersecurity maturity and preparedness, optimize program cost and productivity, and ensure safe, secure AI adoption.

“The 2026 Healthcare Cybersecurity Benchmarking Study is a vital resource for AHA members and a shared commitment to strengthening the entire health sector,” said John Riggi, National Advisor for Cybersecurity and Risk at the American Hospital Association. “Criminal and nation state-supported bad actors are becoming increasingly aggressive, targeting third-party mission- and life-critical systems and putting patient safety in the crosshairs. Hospitals and health systems will benefit from the important and urgent actionable insights from the Benchmarking Study to harden defenses, strengthen resilience, and build the sector’s collective capacity to withstand and recover from such attacks.”

Participating organizations in the 2026 Benchmarking Study get no-cost access to:

Enterprise assessments and peer benchmarks for:
NIST Cybersecurity Framework 2.0 (CSF 2.0)
NIST AI Risk Management Framework (AI RMF)
Organizational Metrics on cyber program ownership, cost, and productivity
HHS Healthcare & Public Health Cybersecurity Performance Goals (HPH CPGs)
405(d) Health Industry Cybersecurity Practices (HICP 2023)

Executive Summary and Deep Dive Reports, to be published in early 2026

Board-ready dashboards and reporting to support cybersecurity investment planning

Peer group comparisons across operational metrics such as ‘cybersecurity expense as a percentage of IT budget’

Benchmarking results and peer comparisons are available immediately upon completion of the assessments.

“The Scottsdale Institute is honored to support the 2026 Healthcare Cybersecurity Benchmarking Study, which is essential to strengthening the trust, safety, and resilience of our healthcare system,” said Janet Guptill, President and CEO of the Scottsdale Institute. “Cybersecurity is no longer a technical challenge, it is a shared responsibility that directly impacts organizational performance, care operations, and patient safety. By participating in the Benchmarking Study, healthcare leaders – from CISO to CEO to the Board – gain the insights and peer collaboration needed to address threats to our critical infrastructure, safeguard the delivery of care, and ensure our industry can adapt and thrive in an evolving digital landscape.”

Participation in the 2026 Benchmarking Study is open to a broad set of organizational types across the health sector, including: Healthcare Delivery Organizations (HDOs), Payers, Healthcare Technology Vendors, Pharmaceutical and Lab Companies, Public Health Organizations, Medical Device Manufacturers, Mass Fatality Management Services, and Federal Response & Program Offices.

“Health-ISAC is proud to co-sponsor the 2026 Healthcare Cybersecurity Benchmarking Study, which delivers unmatched visibility into the risks shaping the health sector’s cyber readiness,” said Errol Weiss, Chief Security Officer of Health-ISAC. “By benchmarking against recognized security practices like NIST CSF 2.0 and HICP, and integrating emerging frameworks such as the NIST AI RMF for stronger AI governance, the study delivers timely, actionable intelligence. These insights help members adapt to evolving threats, including those accelerated by AI, and strengthen their ability to detect, respond to, and recover from incidents that could disrupt patient care.”

Through anonymized data opt-in by participants, analysis from the first two waves of The Benchmarking Study served as a primary input into the Hospital Cyber Resiliency Initiative Landscape Analysis, a key report published by the U.S. Department of Health and Human Services (HHS) in May 2023. In turn, this report helped inform the Healthcare and Public Health Cybersecurity Performance Goals, issued by HHS in January 2024 and proposed as federal minimum cybersecurity standards for the health sector.

“The Health Sector Coordinating Council is honored to sponsor the 2026 Healthcare Cybersecurity Benchmarking Study at a time when rapid AI adoption and increasingly aggressive cyber threats are converging on healthcare’s most critical functions,” said Greg Garcia, Executive Director of the Health Sector Coordinating Council Cybersecurity Working Group. “From clinical care delivery to supply chain operations, the systems that sustain patient safety are now prime targets. This study offers a clear view of sector-wide readiness, helping organizations identify gaps, strengthen defenses, and build the resilience needed to protect essential healthcare services from disruption.”

“The 2026 Healthcare Cybersecurity Benchmarking Study reinforces a critical truth: protecting patient care requires engagement from clinical teams, administrative leaders, and public health professionals alike,” said Leanne H. Field, Ph.D., M.S., Clinical Professor and Director, Leadership in Healthcare Cyber Risk Management professional education program at The University of Texas at Austin. “The Benchmarking Study also serves as a robust, community-led educational pillar for today’s and tomorrow’s hospital leaders, shaping the cybersecurity healthcare risk management curriculum we’ve pioneered at UT Austin. Through dedicated courses on robust risk analysis, business continuity, disaster preparedness, and third-party risk management, all critical challenges consistently identified in past Benchmarking Studies, we’re better preparing healthcare leaders in all disciplines to understand the drivers of risk, make strategic decisions, and strengthen resilience across the industry.”

To participate in the 2026 Benchmarking Study, contact: benchmarks@censinet.com.

About Censinet
Censinet®, based in Boston, MA, takes the risk out of healthcare with Censinet RiskOps, the industry's first and only cloud-based risk exchange of healthcare organizations working together to manage and mitigate cyber risk. Purpose-built for healthcare, Censinet RiskOpsTM delivers total automation across all third party and enterprise risk management workflows and best practices. Censinet transforms cyber risk management by leveraging network scale and efficiencies, providing actionable insight, and improving overall operational effectiveness while eliminating risks to patient safety, data, and care delivery. Censinet is an American Hospital Association (AHA) Preferred Cybersecurity Provider. Find out more about Censinet and its RiskOps platform at censinet.com.

# # #

Justyn Thompson
Censinet
+1 617-221-6875
email us here