Identity Conversation Starters for the Boardroom

For leadership discussion and governance alignment

LexisNexis® RISK SOLUTIONS | Healthcare

About This Reference Guide

This reference guide provides background context and industry perspective to support board-level discussion on patient identity and its role in enterprise trust, risk and digital scale.

It is intended to help frame conversations as healthcare organizations expand digital access, data sharing, analytics and AI. The material focuses on signals leaders are seeing, supported by industry evidence and is not an assessment, benchmark or recommendation.

This reference guide is intended for chief information officers, chief data officers, chief technology officers and senior technology leaders to support executive and board-level discussion. The purpose of this guide is to support governance-level awareness and discussion, not to initiate decisions or remediation.

Leadership Framing and Scope

Leadership use: Recognize identity as a shared enterprise dependency; ensure it is considered in digital growth, AI, interoperability, and mergers and acquisitions; maintain visibility through risk indicators.

For purposes of board-level discussion, this guide uses "identity" as an enterprise-level concept spanning access, authentication, and data trust, not as a reference to a single identity system or function

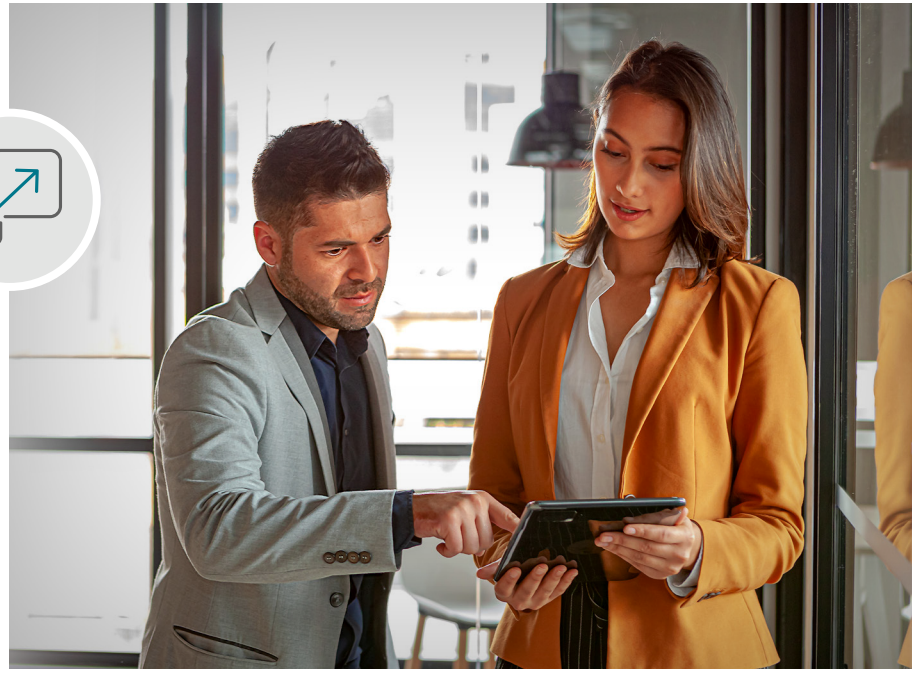
Scale and Prevalence

Risk Focus: Identity errors at healthcare scale are common and magnify with system growth.

Evidence Snapshot

Large healthcare organizations consistently report material patient matching and duplication issues, particularly as systems expand through mergers, acquisitions and multi-system environments.

- Some hospitals have reported record duplicate **rates exceeding 20% in certain environments**, especially where data governance is weak or systems are fragmented.[1] However, most hospitals are operating with a duplicate record rate of 10%.[2]
- One survey found that identification errors in the EHR were common, leading to injury and death.[2] Additionally, diagnostic errors have been found to account for 10% of all patient deaths and 17% of adverse events.[3]
- Patient matching accuracy **decreases as data is shared across organizations**, increasing errors. Duplicate records cause on average $1,950 per inpatient stay and $1,700 per emergency department visit.[4]



Directional Risk Signal — Scale and Prevalence

Contained: Identity issues isolated and corrected locally.

Elevated: Identity inconsistencies increase with acquisitions or digital expansion.

Material: Identity errors impact patient safety, access or data confidence.

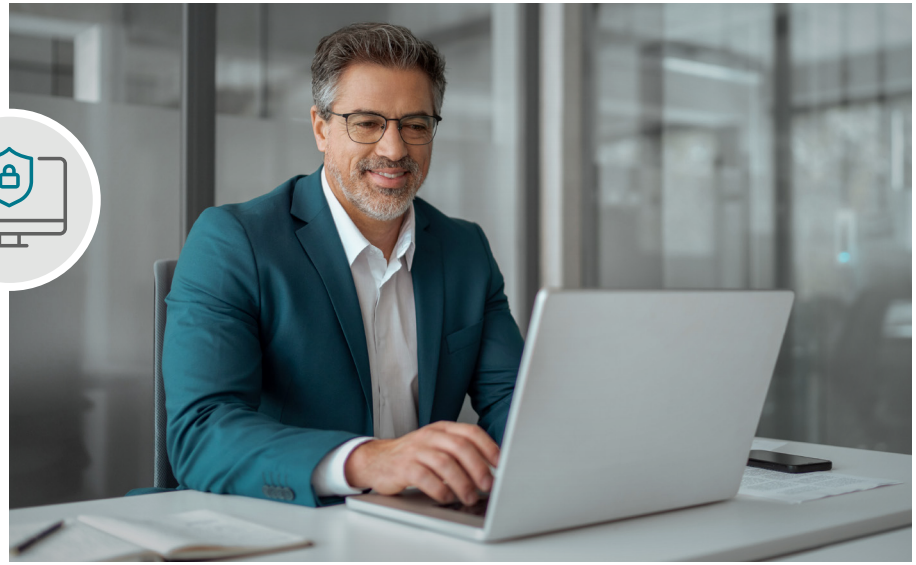
Cybersecurity and Financial Exposure

Risk Focus: Identity reliability directly affects security posture and financial integrity.

Evidence Snapshot

Patient identity reliability increasingly affects enterprise risk through cybersecurity exposure and financial leakage rather than isolated workflow failure.

- More than seven hundred large healthcare data breaches are reported annually, with the average breach costing ~$9.8 million—placing cybersecurity squarely in enterprise financial risk.[5]
- Threat actors increasingly target identity and access controls before authentication, bypassing traditional security measures.[6]
- Ransomware incidents routinely disrupt operations for weeks, with downtime losses averaging nearly $2 million per day and multi-billion dollar sector impact.[7]



Directional Risk Signal — Cyber and Financial

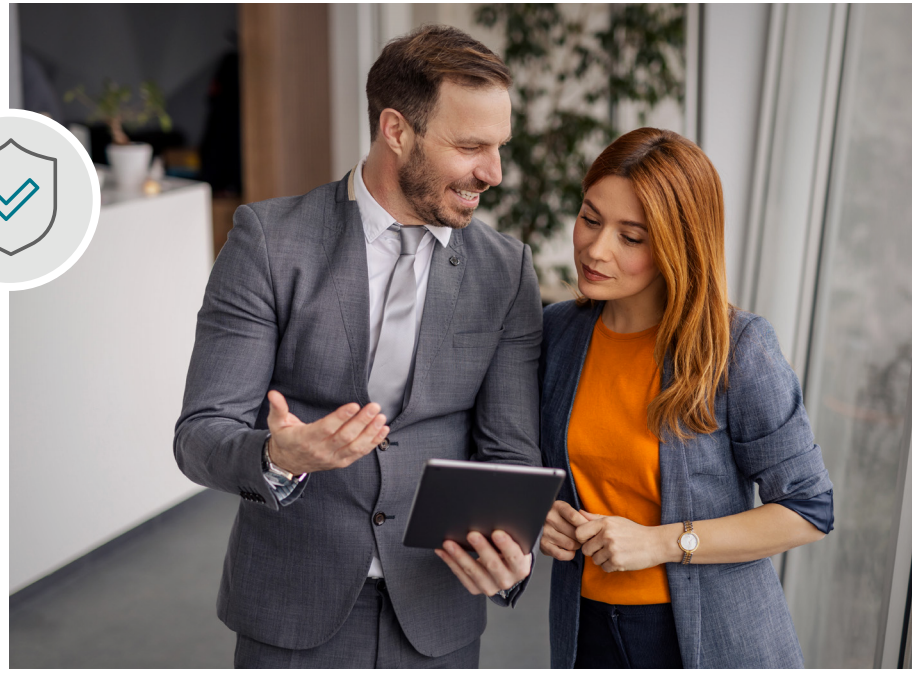
Contained: Identity-related weaknesses rarely surface in security incidents or access control failures.

Elevated: Identity weaknesses increasingly contribute to unauthorized access, account misuse or fraud attempts at digital entry points.

Material: Identity compromise becomes a primary pathway for cyber incidents, materially increasing breach exposure and response impact.

Data Trust, AI Readiness and Governance

Risk Focus: Identity integrity underpins data trust, analytics credibility and AI oversight.



Evidence Snapshot

Patient identity integrity underpins enterprise data trust and becomes more critical as organizations scale analytics, interoperability and AI initiatives.

- National and industry studies consistently identify **patient matching as a foundational barrier to reliable interoperability and trusted data exchange** at scale.[8]
- Research demonstrates that analytics and AI systems **amplify underlying data quality and identity issues**, rather than correct them, increasing decision risk when identity integrity is weak.[9]
- Federal policy efforts increasingly focus on **identity and patient matching accuracy** as prerequisites for nationwide interoperability.[10]

As healthcare organizations expand analytics and artificial intelligence initiatives, weaknesses in identity integrity increasingly propagate across models and decision systems rather than being contained.

Directional Risk Signal — Data and Governance

Contained: High confidence in dashboards and reporting.

Elevated: Manual validation required before analytics.

Material: Leadership doubts data reliability or AI outputs.

How This Maps to Enterprise Risk Oversight

Risk Name:
Patient Identity Reliability Risk

Risk Category:
Enterprise Technology, Data Governance, Cyber Risk

Risk Statement:
Patient identity reliability has emerged as an enterprise level risk. Failure undermines data trust, cybersecurity posture, digital access reliability and financial integrity as healthcare organizations scale interoperability, analytics and AI.

End Notes

1. Medical Economics, “Why Duplicate and Mismatched Patient Records Are a Bigger Problem Than You Think.” medicaleconomics.com
2. Journal of AHIMA, “Double Trouble: Using Health Informatics to Tackle Duplicate Medical Record Issues.” journal.ahima.org
3. National Library of Medicine, National Center for Biotechnology Information, “Patient safety and healthcare quality of U.S. laboratory developed tests (LDTs) in the AI/ML era of precision medicine.” pmc.ncbi.nlm.nih.gov
4. Patient Safety & Quality Healthcare, “A National Patient Identifier Is Up for Debate. Patient Safety Is Not.” psqh.com
5. Healthcare Dive, “Average cost of healthcare data breach nearly $10M in 2024: report.” healthcaredive.com
6. Microsoft, “Defending against evolving identity attack techniques.” microsoft.com
7. HFMA, “Ransomware attacks cost healthcare organizations $21.9 billion in downtime.” HFMA.org
8. Pew Charitable Trusts, “Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records.” pew.org
9. National Library of Medicine, National Center for Biotechnology Information, “Digital Health Data Quality Issues: Systematic Review.” pmc.ncbi.nlm.nih.gov
10. U.S. Centers of Disease Control and Prevention, “Implementing Public Health Interoperability.” cdc.gov

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., registered in the U.S. or other countries. Copyright © 2026 LexisNexis Risk Solutions. NXR17100-00-0526-EN-US

LexisNexis® RISK SOLUTIONS | Healthcare