Health Data, Privacy & Vendor Governance Assessment

Artifact 6 | NorthStar Health Network

NorthStar Health Network is a fictional regional health system comprising 12 hospitals, 70 outpatient facilities, approximately 18,000 employees, and roughly 3 million annual patient encounters. All systems, metrics, incidents, vendors, and findings in this portfolio are simulated.

Scope

Assess data provenance, PHI handling, vendor access, retention, secondary use, security, and patient-facing transparency for NorthStar AI systems. This document is a governance assessment, not legal advice.

Data Governance Assessment

System	Primary data	Key data risk	Required control
Sepsis Prediction	Vitals, labs, meds, demographics, encounter history	Broad PHI; stale or missing data can also create safety risk	Document lineage; role-based access; minimum necessary; quality checks; retention and versioning
Radiology Prioritization	Imaging + metadata	Vendor access; re-use of images; hidden preprocessing changes	BAA / DPA review; secondary-use restriction; change notice; data-deletion evidence
Patient Portal Chatbot	Portal text, account context, approved knowledge	Sensitive disclosure; prompt injection; unsafe retention	PHI-safe architecture; logging controls; limited retention; human escalation; no training on patient data without approval
Clinical Note Summarizer	Longitudinal clinical record	Over-collection; hallucinated synthesis; copy-forward risk	Minimum context; provenance links; clinician verification; audit logs; no autonomous filing
Employee GenAI Assistant	Internal content	Staff may paste PHI into unapproved tool	Technical DLP; approved tool list; training; block uploads / connectors where needed

Vendor Data Due-Diligence Questions

- Does the vendor receive, maintain, or transmit ePHI? If so, is a Business Associate Agreement required and in place?
- Is patient data used to train, fine-tune, benchmark, or improve models beyond NorthStar's approved purpose?
- Where is data stored and processed, and which subprocessors have access?
- What are retention and deletion periods, including backups and derived data?
- Can NorthStar obtain audit logs and evidence of deletion?
- How are security incidents and material model changes reported?
- Can NorthStar exit without losing access to records, logs, or required evidence?

Privacy / Data Decision Gates

Gate	Minimum evidence
Before pilot	Data-flow diagram; lawful / permitted use basis; vendor/BAA review where applicable; security assessment; retention plan; access model
Before production	Validated interfaces; audit logging; patient-facing transparency where applicable; secondary-use restrictions; breach/incident process
Material change	Updated data-flow review; new data category approval; vendor change assessment; revalidation if data meaning or preprocessing changes

Reference basis

HIPAA Privacy and Security requirements apply based on NorthStar’s status and the role of each vendor or service. ONC HTI-1 transparency requirements may apply where predictive decision support is implemented through certified health IT. Applicability is system-specific.