Bryant Lister

Vice President of Data Strategy, Trella Health

bryant@bryantlister.com 503-708-2126

Eugene, Oregon linkedin.com/in/bryantlister

bryantlister.com

STAR FRAMEWORK RESPONSES BRYANT LISTER | TRELLA HEALTH VP OF DATA STRATEGY

Response 1: Building Data Governance from Nothing

Question: Tell me about a time you had to build data governance from the ground up in a rapidly scaling organization.

Situation: L.A.B. Golf had just received private-equity investment and was scaling from a regional manufacturer toward a national brand. There was no enterprise data strategy, no governance framework, no stewardship model, and no accountability for how data was created, stored, or used across ERP, CRM, e-commerce, and analytics platforms.

Task: I was recruited as Vice President of Information Technology to build the entire enterprise information capability, including data strategy, governance, architecture, and responsible AI controls, while supporting a $200M revenue target and private-equity reporting requirements.

Action: I established the company's first Technology Steering Committee with cross-functional executives from Finance, Manufacturing, Sales, Operations, and Marketing. I defined decision rights, stage gates, and portfolio governance. I built enterprise data ownership and stewardship across all business units, developed shared definitions, metadata practices, information classification, and lifecycle standards. I created a responsible AI governance framework covering use-case intake, acceptable use, privacy review, vendor assessment, data quality validation, human oversight, and documented business outcomes. I directed a $3M+ technology portfolio and governed all system integrators and managed providers.

Result: The company moved from ad-hoc data management to a governed, scalable platform architecture. Executive dashboards provided real-time visibility into inventory, sales, and financial performance. The AI governance framework allowed the company to pilot predictive analytics without exposing the organization to uncontrolled risk. Private-equity reporting requirements were met with auditable data lineage and quality metrics.

Response 2: Leading Through a Major Healthcare Data Breach

Question: Tell me about a time you led through a significant data security or privacy crisis.

Situation: During my tenure at the Oregon Health Authority, the organization experienced a major healthcare data breach involving sensitive protected health information. The incident required immediate coordination across executive leadership, legal, privacy, security, communications, program operations, law enforcement, and federal stakeholders.

Task: I was appointed Interim Chief Information Risk Officer and incident commander. My responsibility was to contain the breach, coordinate the multi-stakeholder response, remediate control gaps, and restore organizational trust and regulatory standing.

Action: I immediately established an incident command structure with clear roles for legal, privacy, security, communications, and program leadership. I coordinated with federal regulators and law enforcement while managing internal evidence collection and forensic analysis. I led the development and implementation of the organization's first comprehensive Agency Security Plan, establishing an enterprise roadmap for NIST 800-53-aligned control maturity. I directed corrective-action tracking, evidence development, and executive reporting. I rebuilt operational remediation processes to ensure sustained compliance rather than one-time fixes.

Result: The organization moved from reactive security posture to a governed, measurable control environment. NIST 800-53-aligned controls were implemented and assessed. Executive reporting provided continuous visibility into risk reduction. The breach response became a catalyst for enterprise-wide governance improvement that outlasted the incident itself.

Response 3: Aligning Cross-Functional Stakeholders Around Complex Data Strategy

Question: Tell me about a time you had to align multiple functions around a complex data strategy in a regulated environment.

Situation: At the Oregon Health Authority, enterprise data strategy touched Medicaid, Coordinated Care Organizations, public health, behavioral health, long-term services, legal, privacy, compliance, security, finance, procurement, and vendor management. Each function had its own definitions, priorities, and legacy systems. Data quality was inconsistent, stewardship was unclear, and executive visibility was limited.

Task: I needed to build a unified data strategy and governance model that satisfied regulatory requirements, enabled program delivery, and provided executive leadership with trustworthy information for decision-making.

Action: I developed governance frameworks for data ownership, stewardship, metadata, business definitions, information classification, quality, privacy, retention, access, and lifecycle management. I established governance councils with cross-functional representation and clear decision rights. I created portfolio reporting, KPIs, and roadmaps that translated legislative and regulatory requirements into measurable delivery outcomes. I partnered directly with C-suite, product, and engineering leaders to ensure architecture decisions aligned with business and compliance needs.

Result: Enterprise information quality improved measurably. Executive dashboards and governance councils provided sustained visibility and accountability. Complex healthcare transformation portfolios up to $15M were delivered with regulatory alignment and cross-functional buy-in. The data strategy outlasted individual projects and became embedded in organizational operating models.

Response 4: Implementing Responsible AI Governance

Question: Tell me about a time you built or improved AI governance in an organization that was adopting machine learning or artificial intelligence.

Situation: At L.A.B. Golf, the organization was rapidly adopting AI and predictive analytics to support inventory forecasting, customer personalization, and pricing optimization. There was no governance framework, no oversight mechanism, and no documented process for evaluating whether an AI use case was acceptable, safe, or aligned with privacy and security requirements.

Task: I needed to build a responsible AI governance framework that enabled innovation while controlling risk, protecting customer and business data, and satisfying private-equity oversight requirements.

Action: I designed a framework connecting use-case intake, acceptable use policies, privacy review, security assessment, vendor due diligence, data quality validation, human oversight requirements, documentation standards, and measurable business outcome tracking. I embedded this framework into the Technology Steering Committee governance model, ensuring no AI model moved to production without documented approval. I trained business unit leaders on how to submit use cases, what data quality evidence was required, and how to define human-in-the-loop controls.

Result: The company was able to deploy predictive inventory and customer analytics with documented governance, auditable approval chains, and clear outcome metrics. Private-equity due diligence showed a controlled AI environment rather than an ungoverned experiment. The framework became the template for how the organization evaluated all new data-driven capabilities.