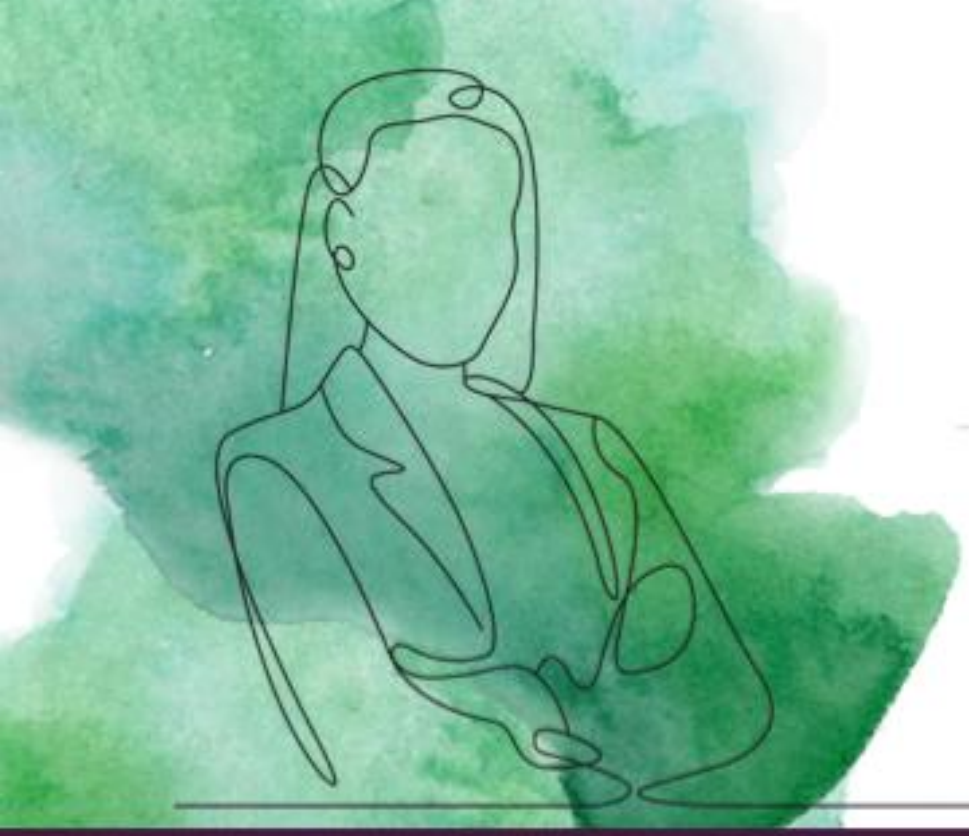

RUDISH HEALTH

Leadership Profile

Executive Director of IT Security and Chief Information Security Officer (CISO)

JPS Health Network
Fort Worth, Texas

Table of Contents

Opportunity	3
JPS Health Network	4
Reporting Structure	5
Position Summary	6
Candidate Qualifications	8
Compensation	10
Tarrant County & Fort Worth, Texas	10

Position	Executive Director of IT Security and Chief Information Security Officer
Organization	JPS Health Network
Location	Fort Worth, Texas
Website	www.jpshealthnet.org

Opportunity

JPS Health Network, a publicly funded health network serving Tarrant County in North Texas, is seeking an accomplished cybersecurity executive as its next Executive Director of IT Security and Chief Information Security Officer (CISO). This newly created role will establish information security as an independent function with a dedicated executive owner.

Reporting to the Senior Vice President, Chief Information Officer, with an additional reporting line to the Chief Executive Officer, the CISO will serve as JPS's HIPAA Security Official and enterprise-wide owner of cybersecurity strategy, governance, architecture, operations, identity and access management, data protection, incident response, and third-party risk management. Key priorities include: (1) developing and executing a multi-year information security roadmap, including a full assessment of current tooling and vendor relationships; (2) maturing governance, audit readiness for NIST and HIPAA, and executive- and Board-level reporting; (3) building and leading the security organization, including close partnership with JPS's IT Risk Manager; and (4) managing vendor relationships for outsourced security services, such as a Security Operations Center or Managed Security Service Provider, alongside direct people leadership.

The successful candidate brings direct healthcare cybersecurity experience, ideally within a large, complex health system, along with an understanding of the unique risk, compliance, and funding considerations that distinguish a public, safety net academic medical center from other environments. Internally, this leader will interact regularly with the Chief Executive Officer, executive leadership, and the Board of Managers, and must operate seamlessly and credibly at that level. JPS is seeking a leader who can assess the organization's needs, bring expertise to the procurement and decision-making rhythms of a government-affiliated entity, and commit to working on-site in Fort Worth. The CISO will make a lasting impact within this uniquely positioned health system.

JPS Health Network

The Tarrant County Hospital District, known as JPS Health Network, is a trusted healthcare leader in Tarrant County, delivering compassionate, high-quality care to all who need it, regardless of insurance status or ability to pay. With a 582-bed hospital, more than 25 community-based clinics, and a team of over 7,200 professionals, JPS provides comprehensive services that include a level 1 trauma center, behavioral health, maternal and neonatal care, primary and specialty medicine, and more. As the county's largest teaching and medical training institution and the most comprehensive provider of behavioral health services, JPS stands at the intersection of access, innovation, and community trust. Governed by an 11-member Board of Managers, JPS is committed to high-quality care, community well-being, and medical innovation, and it is a three-time recipient of the Gallup Exceptional Workplace Award, a global recognition for organizations that foster extraordinary workplace engagement, innovation, and performance.

JPS Health Network traces its origins to October 1877, when future Fort Worth mayor John Peter Smith donated five acres of land at what is now 1500 South Main Street for a community medical facility. A hospital affiliated with the Fort Worth Medical College opened in 1906, and in 1913 Tarrant County commissioners agreed to match city funding for a combined city-county hospital, which opened with 25 beds. Construction of a new 166-bed City-County Hospital began in 1938 on the land Smith had donated, and the facility served as the region's primary trauma center through the polio epidemic and beyond. The hospital was renamed John Peter Smith Hospital in 1954, and the Tarrant County Hospital District was established in 1959 to provide a dedicated funding structure for the organization.

Following decades of expansion through the 1970s and 1980s, JPS extended its footprint into the community through a network of health centers established across Tarrant County in the 1990s. Today, the Main Street campus has grown into a hospital licensed for 582 beds, supported by a five-story acute care Patient Care Pavilion, an outpatient care center, and a dedicated psychiatric services facility, continuing to serve Tarrant County's healthcare and access needs.

Today, JPS is building on that legacy through the largest expansion in its history. The JPS Master Facility Plan is a transformative investment in the future of healthcare in Tarrant County, expanding and modernizing facilities across the network to meet the needs of a growing community. The multi-year plan will enhance access to care, strengthen critical services, and create modern environments designed to support patients, team members and the next generation of care.

2025 Key Statistics

For additional information, please visit the *JPS Report to the Community*

System: 582 bed hospital; 25+ clinics
Community Health Visits: 691,359
ED Visits: 162,848
Total Surgeries: 17,607
Patient Days: 190,044
Urgent Care Visits: 44,606

Team Members: 7,200+
Nurses: 2,450+
Physicians: 580+
Medical Staff and APPs: 1,330+
Residents and Fellows: 250+

Source: JPS Health Network, About JPS Facts and Figures

Mission, Vision, and Values

Mission
Transforming healthcare delivery for the communities we serve.

Vision
To be a regional and national leader in improving the patient and family experience, improving the quality and outcomes of population health, and improving access to care.

Values
Trust, Mutual Respect, Excellence, Integrity, Accountability, Teamwork.

Awards and Recognitions

JPS Health Network has earned the trust of its patients, the validation of respected accrediting bodies, and recognition from professional and community organizations. From trauma care to stroke response and from nursing excellence to workplace culture, these honors reflect the organization's commitment to the highest standards of safety, quality, and performance.

Reporting Structure

The CISO will report to JPS Health Network's Senior Vice President, Chief Information Officer, with a dotted-line reporting relationship to the Chief Executive Officer given the strategic importance of this newly established role. The Executive Vice President and Chief Financial Officer maintains executive oversight of the IT organization.

Supervisory Role

This role directly leads a team of six to eight FTEs, including a Manager of IT Security and a Manager of Identity & Access Management, and holds budget and vendor management responsibility for outsourced security services (e.g., a Security Operations Center or Managed Security Service Provider), in addition to internal staff.

Position Summary

The CISO provides strategic leadership for JPS Health Network's enterprise information security and cyber resilience program. This role serves as the organization's HIPAA Security Official and is accountable for cybersecurity strategy, governance, architecture, operations, identity and access management, data protection, incident response, regulatory compliance, and third-party risk management. The CISO leads the information security organization, partners across clinical and business functions, and advises executive leadership and the Board of Managers on cybersecurity risk and resilience. The incoming CISO will inherit a stabilized technical foundation with meaningful room to shape multi-year tooling, governance, and staffing decisions.

Primary Duties and Responsibilities

- Develops and executes the enterprise information security strategy and multi-year roadmap, and defines JPS's cybersecurity risk appetite in coordination with executive leadership and the Board; ensures alignment with clinical, operational, and financial priorities.
- Establishes and maintains the information security governance framework covering policies, standards, procedures, exceptions, and control ownership, and directs alignment with the NIST Cybersecurity Framework, NIST 800-53, and HITRUST.
- Serves as the designated HIPAA Security Official with overall final responsibility for the security of electronic protected health information.
- Reports information security posture, risk, and program performance to the CEO, SVP Chief Information Officer, executive leadership, and Board, and leads ongoing cybersecurity education to strengthen executive and Board risk literacy.
- Partners with the IT Security Risk Manager in the Office of Legal Affairs as the independent second-line risk oversight function, receives independent risk review findings, and drives remediation to closure.

- Directs security architecture across cloud, on-premises, hybrid, and as-a-service environments and owns the Zero Trust roadmap across identity, network, workload, endpoint, and device domains.
- Directs the enterprise Identity and Access Management program through the IAM Manager, including role-based access, access certification, multi-factor authentication, single sign-on, and Privileged Access Management.
- Directs security operations, security engineering, endpoint protection, vulnerability management, patch management, threat detection, and coordination with Managed Security Service Providers through the Security Manager.
- Directs enterprise data protection strategy covering classification, encryption, key management, Data Loss Prevention, backup and recovery security controls, and controls for inter-organization, intra-organization, and extra-organization clinical data movement.
- Directs the insider threat program and partners with the Office of Legal Affairs, Compliance, and Research on data governance for secondary data use, analytics, and artificial intelligence model training.
- Owns the enterprise cybersecurity incident response program including plan development, playbook maintenance, tabletop and functional exercises, and leads the technical response to active incidents in partnership with the Office of Legal Affairs, which owns HIPAA breach notification to the Office for Civil Rights and affected individuals.
- Partners with Clinical Operations and IT Infrastructure to validate downtime procedures, disaster recovery readiness, and cyber-related business continuity plans so that patient care continues during technology disruptions and informs Due Care standards for the cyber insurance program managed by the Office of Legal Affairs.
- Owns compliance with the HIPAA Security Rule and applicable HIPAA Privacy Rule provisions, HITECH, HHS, CMS, and OCR enforcement guidance, and ensures adherence to Texas privacy and data protection laws including the Texas Medical Records Privacy Act.
- Owns the third-party information security risk program including vendor tiering, security assessment methodology, ongoing monitoring, and remediation thresholds, and partners with the Office of Legal Affairs on Business Associate Agreements and Right to Audit contract terms.
- Partners with Enterprise Risk Management to translate cybersecurity risk into the enterprise risk framework, with Biomedical Engineering and Clinical Engineering on connected medical device and Internet of Things security, and with Clinical Informatics, Nursing Informatics, and Medical Informatics on security controls in the EHR and ancillary clinical systems.
- Owns the information security risk register including risk identification, quantification, treatment planning, and executive reporting, and establishes leading and lagging indicators for cybersecurity program performance.

- Builds, leads, and develops the information security organization and partners with Human Resources on cybersecurity workforce planning.
- Represents JPS externally within industry communities such as H-ISAC.
- Prepares concise reports for executive leadership, Board of Managers, and stakeholders regarding emerging security policy issues.
- Prepares department operating budgets on an annual basis and monitors areas of responsibility for compliance within the current budget; develops cost estimates, forecasts, and expenditures to optimize rewards mix and ensures good governance and compliance processes.

Candidate Qualifications

Education and Experience

- Bachelor's Degree in Cybersecurity, Information Systems, Computer Science, Business Administration, Health Informatics, or related field of study from an accredited college or university.
- Advanced degree preferred.
- CISSP or CISM certification required; HCISPP or CRISC preferred.
- 10 or more years of information security experience; to include experience protecting complex clinical, business, and infrastructure environments in a healthcare setting, operating within a county, public, academic, safety net, or federally qualified health center environment, and experience building or maturing a security program with full budget accountability.
- 5 or more years of progressive leadership experience working in an information security role within a healthcare provider, health system, academic medical center, or similarly regulated environment; to include experience leading enterprise incident response for a material cybersecurity event.
- Experience building or maturing a security program with full budget accountability, including management of outsourced security vendors (e.g., SOC, MSSP), is preferred.
- Experience supporting executive leadership and cross-functional strategic initiatives is preferred.
- Experience with a greenfield or major capital facility technology security build
- Experience leading a Zero Trust program from strategy through operational execution.
- Experience securing a connected medical device and Internet of Medical Things environment at scale.
- Experience presenting cybersecurity risk to a Board of Directors or Board-level risk committee.
- Active membership or leadership role in the Health Information Sharing and Analysis Center (H-ISAC).

Knowledge, Skills and Abilities

- Knowledge and ability to manage a multi-million dollar information security operating and capital budget.
- Advanced knowledge of enterprise cybersecurity strategy in a regulated healthcare environment.
- Advanced knowledge of the HIPAA Security Rule, HIPAA Privacy Rule, HITECH, HHS, CMS, and OCR enforcement mechanisms.
- Advanced knowledge of the NIST Cybersecurity Framework, NIST 800-53 control set, and HITRUST.
- Knowledge of the three lines of defense model and the ability to operate as the first-line security program owner while partnering constructively with independent second-line risk oversight.
- Knowledge of Texas privacy and data protection laws, including the Texas Medical Records Privacy Act.
- Knowledge of Texas Health Services Authority, TX-RAMP, and state-level health data requirements.
- Knowledge of security architecture across cloud, on-premises, hybrid, and as-a-service environments.
- Knowledge of connected medical device and Internet of Things security in partnership with Biomedical Engineering.
- Knowledge of Microsoft Office Suite (Excel, Word, Outlook, and PowerPoint).
- Skilled in translating cybersecurity risk, financial impact, and performance metrics into business, clinical, and financial terms for executive leadership, the CFO, and the Board.
- Skilled in leading enterprise incident response for a material cybersecurity event.
- Skilled in communicating, coaching, and providing feedback effectively to individuals at all organizational levels and across diverse educational and cultural backgrounds.
- Ability to build trusted relationships and communicate effectively with physicians, clinical leadership, front-line staff, supervisors, and hospital personnel regarding cybersecurity risks and controls that affect patient care.
- Ability to perform effectively under pressure, including during active cybersecurity incidents, while managing multiple competing priorities and maintaining attention to detail.
- Ability to plan, organize, direct and control the operations of a critical function and effectively delegate managerial responsibilities to qualified managers and staff.
- Ability to recruit and retain competent staff utilizing coaching skills that will foster employee development, productivity, growth, satisfaction, loyalty, commitment and teamwork.

- Ability to maintain a high level of confidentiality and professionalism in working with sensitive and personal information.
- Willingness to work on-site in Fort Worth, Texas.

Compensation

An attractive compensation, bonus, benefits, and relocation package will be offered commensurate with the candidate's experience. Additional benefits include 30 days of PTO (inclusive of holidays) and a 5% employer match on the retirement plan.

Tarrant County & Fort Worth, Texas

Tarrant County, anchored by the City of Fort Worth, is one of the fastest-growing regions in the country, with a population of more than 2.2 million residents and continued gains driven by both natural growth and steady in-migration. Fort Worth itself is the fifth-largest city in Texas and among the 15 largest in the nation, with a diverse population of more than 960,000. Known nationally as "Cowtown," the city has built a reputation as a major economic engine for North Texas, built on aerospace and defense, transportation and logistics, and a growing base in healthcare, finance, and professional services. The region also benefits from no state personal income tax and a cost of living below that of many major U.S. metros.



Historic Stockyards



Fort Worth Water Gardens

Fort Worth is defined by both frontier heritage and world-class culture. The Fort Worth Stockyards National Historic District preserves the city's cattle-trading legacy with a twice-daily longhorn cattle drive down brick-paved Exchange Avenue, alongside western shops, saloons, and rodeo tradition. A few miles away, the Cultural District brings together an unusual concentration of architecturally

significant museums for a city of this size: the Kimbell Art Museum, the Modern Art Museum of Fort Worth, and the Amon Carter Museum of American Art, each designed by a Pritzker Prize-winning architect. Downtown, Sundance Square offers 35 walkable blocks of restaurants, shops, and entertainment centered on Bass Performance Hall, home to the Fort Worth Symphony, opera, and ballet. Outdoor life is equally accessible, with the Fort Worth Zoo consistently ranked among the nation's best, the Fort Worth Botanic Garden's 2,500 plant species, and more than 100 miles of Trinity Trails connecting the Stockyards, downtown, and the Zoo along the river.

The region is home to respected institutions of higher education, including Texas Christian University, the University of Texas at Arlington, and Tarrant County College, supporting a strong talent pipeline and vibrant college-town energy around neighborhoods like TCU's campus district. Families are drawn to the area's combination of value and lifestyle: median home prices in Fort Worth run well below those in Dallas and many North Texas suburbs, while communities such as Keller, Southlake, and North Richland Hills offer highly rated school districts alongside larger lots and newer construction. Dallas-Fort Worth International Airport provides direct global connectivity, making both business travel and family visits easy from nearly anywhere in the country.



Fort Worth

With its blend of authentic Western character, nationally recognized arts and culture, strong economic fundamentals, and relative affordability, Fort Worth and Tarrant County offer a quality of life rarely found in a single place, and a community where new residents quickly feel at home.

Contact

Rudish Health
www.rudishhealth.com



Rick Schooler
Advisor
Telephone: (407) 761-3052
E-mail: rick@rudishhealth.com



Megan Kolodgy
Vice President
Telephone: (734) 276-3253
E-mail: megan@rudishhealth.com



Nicole Brown
Senior Director
Telephone: (412) 352-3848
E-mail: nicole@rudishhealth.com



Laura Yancone
Manager, Talent Leadership Services
Telephone: (585) 507-6799
E-mail: laura.yancone@rudishhealth.com