		JOB CODE: 4	
POSITION TITLE:	Director, IT & Network Security	**DATE:**	April 2019
DIVISIONS:	IT		
REPORTS DIRECTLY TO:	Chief Financial & Security Officer		

FULCRUM HEALTH:

Fulcrum Health, Inc. is a nonprofit, physical medicine and pain management organization that has delivered quality care through its network of over 2,500 licensed and credentialed chiropractic and acupuncture service providers for over 35 years. Our product offerings include acupuncture and chiropractic pain management services and we serve over 1.7 million health plan members within the Upper Midwest, Fulcrum continues to offer innovative and inspiring ways to leverage physical medicine that help lower health care costs, achieve better outcomes, and increase patient satisfaction.

POSITION PURPOSE:

Fulcrum Health is seeking a proactive Director of IT and Network Security to oversee its technology operations and data security program. This individual will work within a dynamic, fast-paced environment where IT regularly engages with other functional areas to support and implement solutions for business needs. To be successful in this role, candidates must be highly motivated, capable of handling continuous learning, proficient at looking for ways to develop new and improved systems, flexible and goal oriented.

ACCOUNTABILITIES:

IT & Network Management (50%)

- Oversee operations of Fulcrum's cloud services provider and coordinate activity among IT service providers. Research, evaluate prioritize, test and coordinate the deployment of new technologies and lead IT vendor selection and supplier contracts process.
- Serve as primary IT point of contact to facilitate solution implementation and system upgrades with third party vendors.
- Perform routine checks and troubleshoot network, workstation and software issues.
- Establish and maintain network user accounts, user environment, directories, security and user access rights for enterprise and Admin users.
- Audit and monitor user access and activity within electronic systems
- Oversee applications, networking and operating systems (installations and upgrades)
    - Ensure that computer and network security patches and service packs have been deployed

    - Configure hardware, ie: computer workstations, telco system as required.
    - Work with third-party IT vendor to ensure that all workstation and network security patches, anti-virus updates and firewall definitions have been deployed and updated.
- Develop, implement and communicate policies and procedures that define enterprise information technology standards and guidelines.

Network and Data Security (50%)

- Serve as technical lead to define and prioritize the implementation of needed security controls across the organization. Regularly review the threat landscape and revise security program operations to address these threats.
- Ensure ongoing monitoring and reporting of access to all network databases, websites and third-party software that house company data.
- Coordinate periodic vulnerability scans and penetration testing with third-party vendor and address remediation items as identified.
- Work with leadership to develop strategies and plans to enforce security requirements and address identified risks.
- Define enterprise security awareness policies and procedures and monitor/audit compliance.
- Provide direct support to the business for security related issues and gaps. Serve as technical lead for development and administration of corporate Disaster Recovery Plan (DRP).
- Serve as lead technical staff during health plan and customer audits as well as lead security due diligence when vetting new vendors and / or hosted solutions.
- Maintain familiarity with internal and external security audit standards and requirements, ie: NIST, HIPAA, etc, to ensure company compliance and readiness.
- Oversee annual Security Risk Assessment (SRA) and lead remediation effort.

REQUIRED QUALIFICATIONS:

- Bachelor's Degree in Computer Science or related field.
- 5-8 years of experience in a management or administrator role focusing upon Windows networks, Windows Servers, Active Directory, Windows Administration and Security.
- 3-5 years of experience focused upon security within a highly regulated industry. Healthcare security experience preferred.
- Experience in a hosted cloud infrastructure required and experience using manage services preferred.
- Experience defining and implementing IT and Network Security policies, procedure and best practices.
- Experience managing the oversight and application of security regulations (HIPAA, NIST, etc.) within a healthcare organization.

- Capability and desire to partner with other functional areas for using technology as a strategy to advance the business and mission.
- Prior experience managing and deploying Sophos security products, Citrix FileShare among others.

DIRECT/INDIRECT REPORTS:
Number of direct reports and titles: 0
Number of indirect reports: 0