THE HEALTH COLLABORATIVE

Administrator, Information Security

Reports to: Director, Information Security		
Level/Grade Professional	**Type of Position** Full Time	**Hours/Week** 40 hrs/week; Exempt

GENERAL DESCRIPTION

The Administrator, Information Security will work with the Director, Information Security as well as the network and server administration team to develop, maintain and operate the company's information security systems. The IS Administrator will be responsible for reviewing monitoring reports and alerts and ensuring that corrective action is completed. They will also be responsible for designing, developing and deploying systems to streamline and automate information security auditing activities using a variety of tools including scripts and MS Office products as well as COTS applications.

JOB RESPONSIBILITIES

- Perform hands-on support for a wide range of security technologies such as SIEM, IDS/IPS, HIDS, DLP, malware analysis and protection, content filtering, logical access controls, identity and access management, vulnerability scanners, and forensics.
- Assist in developing and enforcing policies and procedures to ensure information system security.
- Execution and automation of daily/weekly/monthly reporting.
- Monitor and analyze security alerts and reports and escalate issues to appropriate management.
- Collaborate with technology partners and IT management to remediate security vulnerabilities.
- Support entitlement reviews and remediation of exceptions.
- Participate in information security design quality reviews.
- Understand and enforce general computing controls.
- Support compliance efforts, including validation of security assessments and, test or assessment results, and assist management with the determination of the effectiveness of controls designed and operating in the internal control environment.

POSITION REQUIREMENTS

- Familiarity with the following information security domains:
  - Vulnerability Management
  - Endpoint Security
  - Access Control
  - Telecommunications and Network Security
  - Risk Management
- Must have strong work ethic and time management skills
- Must be detailed-oriented individual
- Must have excellent interpersonal skills
- Must have excellent communications skills, both verbal and written
- Must have excellent customer service skills

EDUCATION/CERTIFICATION REQUIREMENTS

- Associates Degree Information Technology OR CompTIA Network+ OR CompTIA Security+
- Minimum of 1 year experience in related field

OTHER INFORMATION

Preferred skills & experience:

- Experience with various security monitoring and assessment tools, such as DLP, IPS/IDS, etc.
- Familiarity with frameworks such as HITRUST, NIST, ISO 27001/2, etc. and regulations such as HIPAA and HITECH.
- Experience and working knowledge of industry standard security controls and frameworks.
- Security certifications such as SEC+, GSEC, CEH, CISSP, SSCP, or CISM.
- Experience with penetration testing toolsets and attack vector concepts (i.e., NMAP, Burp Suite, Metasploit, Core Impact, etc.).
- Experience with IT infrastructure including desktop endpoints, network, server, data storage technologies.
- Assist in the development and deployment of corporate information security strategy, as well as deployment, administration, configuration and support of security related systems.

APPROVED BY M.Wells, Director, Information Security **DATE POSTED** October 2015

Disclaimer: Nothing in this job description restricts the company's right to assign responsibilities to this job at any time as critical features of this job are subject to change any time.