Director, Privacy and Security Compliance

Tegria RCM
Job Location: Remote
Full Time/Days

JOB SUMMARY:

The Director of Privacy and Security Compliance leads Tegria RCM's privacy and IT security compliance program and supports the Tegria RCM Compliance Officer and the Tegria RCM overall compliance program by administering and implementing privacy and IT security compliance programs, policies, and practices consistent with the Federal Sentencing Guidelines' Seven Elements of an Effective Compliance Program. Assists in coordinating and administering compliance education across the organization. Leads and facilitates compliance with relevant laws, regulations, and frameworks, including but not limited to HIPAA, HITRUST, PCI, Cyber Essentials, SOC2, and applicable state regulations. Serves as the enterprise subject matter expert on privacy laws and regulations. Oversees and manages the planning, implementation, oversight, auditing, monitoring, and ongoing operation of Tegria RCM's privacy and security compliance program. Acts as a compliance liaison to Tegria RCM partners and government agencies as appropriate. Coordinates and leads a risk-based privacy and IT Security compliance auditing and monitoring program based on continuous assessment of the Tegria RCM risk environment. Investigates potential privacy and security compliance violations and recommends appropriate corrective action.

MINIMUM REQUIREMENTS:

- Minimum of 7 years' experience in cross-discipline healthcare privacy and Information Security/Information Technology experience
- Minimum of 5 years' experience in a supervisory role in healthcare privacy, IT security compliance, or combination
- Demonstrated experience with representing security controls to external auditors and/or customers.
- Strong knowledge of healthcare privacy and security compliance, governance, and risk management concepts and practices.
- Strong understanding of common security and privacy standards, regulations, and laws relating to a cloud software development company (e.g., SOC 2, ISO 27001, HIPAA, HITECH, CCPA, HITRUST, etc.).
- Experience developing information privacy, security, and compliance policies, procedures, and supporting documentation.
- Experience conducting information privacy risk assessment/analysis and determining positional breach exposure.
- Experience with evidence gathering, validation, and managing audits for SOC 2 Type 2, and HITRUST certifications.

EDUCATION/LICENSES/CERTIFICATIONS:

- Bachelor's degree in Health Administration, Healthcare Information Systems, Health Information Management or equivalent.
- Privacy and/or IT Security certification, such as CHPC, CISA, CHPS, or equivalent
- Master's degree in Health Administration or other related privacy, security, or medical record management related field (Preferred)

FOR MORE INFORMATION/TO APPLY:

https://jobs.jobvite.com/careers/tegriarcm/job/ow8Fmfwp?__jvst=job%20board&__jvsd