POSITION OVERVIEW

Job Title: Associate Vice President, Privacy
Business Title: *AVP Privacy*
Job Code: SRDIRCL
FLSA Status: Exempt
Department: Compliance
Reports to: Chief Compliance Officer
Location: National - Remote
Draft Date: 05082026
Revision Date:
Approved By: Melissa Ford
Role: People Leader

Job Description: AVP, Privacy

AVP Privacy, Position Summary

The Associate Vice President Privacy is a senior leader responsible for overseeing Radiology Partner's privacy functions relating to HIPAA compliance, patient privacy, technology integration, and risk management. This pivotal role will scale and drive a **privacy** protection program across RP Clinical Practices and Mosaic Clinical Technology division. The AVP Privacy will develop a global privacy program that complies with all data protection las (e.e. GDPR, CCPA) by expanding current policies and procedures, conducting risk assessments and evaluating relevant regulations. The role serves as an organizational authority and SME on healthcare privacy, regulatory affairs, and industry best practices. Reporting to the Chief Compliance Officer, this role collaborates cross-functionally with legal, compliance, IT, security, and clinical teams to safeguard patient data, mitigate privacy risk, and support innovation in radiology technology platforms.

POSITION DUTIES AND RESPONSIBILITIES

1. HIPAA Compliance & Regulatory Oversight

- Lead and oversee HIPAA Privacy Rule compliance as it pertains to patient records, diagnostic images, and electronic protected health information (ePHI) within complex practice environments.
- Monitor, interpret, and disseminate updates in privacy and data laws, regulations, and guidelines affecting radiology and healthcare IT, including federal, state-specific patient privacy statutes, marketing and sale of PHI rules, and international standards.
- Serve as SME on privacy issues, including breach notification, patient complaints, and government audits.
- Develop and maintain privacy policies

2. **Patient Privacy & Security Risk Management**

    - Design, implement, and maintain the organization's privacy risk management program, including regular risk assessments, incident response, and mitigation strategies for legacy and emerging radiology technologies.
    - Collaborate with IT, IT Security, and internal and external development teams to perform privacy impact assessments, support controls for digital imaging and communications in medicine (DICOM), PACS, cloud imaging services, and AI-driven diagnostic tools.
    - Ensure robust controls for data retention, secure disposal of records/image media, authentication, audit trails, access control, encryption, and endpoint/device security in radiology environments.
    - Investigate privacy incidents, coordinate incident response, containment, regulatory notification, root cause reporting, and remediation efforts in the event of PHI exposure or data breach.

3. **Technology Integration & Health IT Compliance**

    - Direct privacy-related technology evaluations and integrations for imaging platforms, EHR interfaces, artificial intelligence (AI)/machine learning tools, cloud repositories, interoperability APIs, and remote access systems.
    - Support evaluation of health IT vendors and partner systems for adherence to privacy, security, and interoperability standards, and applicable FDA medical device cybersecurity guidance.
    - Collaborate with IT and operations to embed privacy-by-design in software/platform development, deployment, and lifecycle management for all radiology-related technology assets.
    - Drive cross-functional collaboration between Compliance, Legal, IT, Security, Clinical, Operations, Human Resources, and Business Development to deliver unified, practical, risk-informed programs.
    - Facilitate or participate in the organization's strategic planning processes for privacy, bringing a privacy risk lens to product development, data monetization, clinical trials, and AI/ML deployments.

4. **Policy Development, Training, and Program Maturity**

    - Support the development, maintenance, and enforcement of privacy, data protection, and acceptable use policies relevant to radiology data and workflows.

- Ensure regular policy reviews and alignment to new legislative/regulatory requirements, technology advancements, and organizational risk posture.
- Design and administer privacy, security, and information governance training programs for clinical, technical, and administrative staff, including compliance expectations for handling, transmitting, and sharing images and related PHI.
- Develop, update, and deliver targeted training on topics such as preventing common privacy incidents, patient image access, audit log reviews, and secure remote imaging interpretation.
- Drive continuous program improvement, periodic gap analyses, internal/external audits, and change management for all privacy initiatives.

5. **Incident Response & Breach Management**
    - Collaborate with IT Security, Compliance, and Legal to establish, maintain, and continually improve incident response procedures and breach notification policies and playbooks in accordance with HIPAA, state, and contractual requirements.
    - Lead the organization's response to privacy incidents, coordinating investigation, communications (internal and external), remediation, regulatory disclosures, and root cause analysis.
    - Serve as a liaison for cross-functional incident response, coordinating with IT Security, Compliance, Legal, Operations, and external vendors.
    - Conduct after-action reviews, implement lessons learned, and direct enterprise-wide improvements to prevent recurrence.
6. **Vendor Risk Management**
    - Oversee assessment, contracting, and ongoing monitoring of vendors, partners, and business associates (including imaging cloud providers, teleradiology, and AI services) for compliance with privacy and security standards.
    - Ensure execution of robust Business Associate Agreements (BAAs), due diligence on vendor controls, periodic audits, and mandatory breach and vulnerability reporting.
    - Develop and apply criteria for vetting new vendors, exits, and remediation plans if privacy or compliance deficiencies are discovered.
7. **People Leader**
    - Promotes communication and cooperation among teammates to create a spirit of unity in the department.

- Works closely with leadership and teammates to improve work relationships, build morale, and increase productivity and retention.
- Provides day-to-day performance management guidance to direct reports (e.g., coaching, counseling, career development, disciplinary actions).

REQUIRED QUALIFICATIONS

Education:

- Bachelor's degree in Health Information Management, Computer Science, Healthcare Administration, Biomedical Informatics, or related field preferred.
- Master's degree or advanced degree (JD, MPH, MBA, MHA, MLIS) preferred.

Certifications:

- Certified Information Privacy Professional (CIPP/US) or comparable privacy certification from IAPP.
- Certified in Healthcare Privacy Compliance (CHPC, HCCA) and/or Certified in Healthcare Privacy and Security (CHPS, AHIMA) are highly desirable.
- Additional certifications in security (e.g., CISSP), compliance (e.g., CHC, CCEP), or healthcare management are assets.

PREFERRED PROFESSIONAL SKILLS AND EXPERIENCE

- Minimum 8–10 years of progressive experience in healthcare privacy, regulatory affairs, international data privacy laws, or compliance required, ideally in a provider, radiology, health system, or health technology/software company.
- At least 5 years in a leadership role managing privacy/compliance programs, including direct oversight of privacy professionals and/or multi-disciplinary project teams.
- Demonstrated expertise in HIPAA Privacy, Security, and Breach Notification Rules; experience with business associate/vendor risk management in healthcare environments.
- Experience designing and implementing privacy programs for clinical workflows, health IT systems, and digital imaging platforms (RIS, PACS, VNA, cloud, EHR).
- Direct experience with incident response management, privacy training development, and managing privacy risks related to cloud, AI, and interoperable workflow environments.

Physical Activities

Ascending or descending ladders, stairs, scaffolding, ramps, poles and the like.

☒ Never ☐ Occasionally ☐ Constantly

Moving self in different positions to accomplish tasks in various environments including tight and confined spaces.

☐ Never ☒ Occasionally ☐ Constantly

Remaining in a stationary position, often standing or sitting for prolonged periods.

☐Never ☐ Occasionally ☒ Constantly

Moving about to accomplish tasks or moving from one worksite to another.

☐ Never ☒ Occasionally ☐ Constantly

Adjusting or moving objects up to 15 pounds in all directions.

☐ Never ☒ Occasionally ☐ Constantly

Communicating with others to exchange information.

☐ Never ☐ Occasionally ☒ Constantly

Repeating motions that may include the wrists, hands and/or fingers.

☐ Never ☐ Occasionally ☒ Constantly

Operating machinery and/or power tools.

☐ Never ☒ Occasionally ☐ Constantly

Operating motor vehicles or heavy equipment.

☐ Never ☒ Occasionally ☐ Constantly

Assessing the accuracy, neatness and thoroughness of the work assigned.

☐ Never ☐ Occasionally ☒ Constantly

Environmental Conditions

Low temperatures.

☐ Never ☒ Occasionally ☐ Constantly

High temperatures.

☐ Never ☒ Occasionally ☐ Constantly

Outdoor elements such as precipitation and wind.

☐ Never ☒ Occasionally ☐ Constantly

Noisy environments.

☐ Never ☒ Occasionally ☐ Constantly

Hazardous conditions.

☐ Never ☒ Occasionally ☐ Constantly

Poor ventilation.

☐ Never ☒ Occasionally ☐ Constantly

Small and/or enclosed spaces.

☐ Never ☒ Occasionally ☐ Constantly

No adverse environmental conditions expected.

☐ Never ☒ Occasionally ☐ Constantly

Physical Demands

Sedentary work that primarily involves sitting/standing.

☐ Never ☐ Occasionally ☒ Constantly

Light work that includes moving objects up to 20 pounds.

☐ Never ☒ Occasionally ☐ Constantly

Medium work that includes moving objects up to 50 pounds.

☒ Never ☐ Occasionally ☐ Constantly

Heavy work that includes moving objects up to 100 pounds or more.

☒ Never ☐ Occasionally ☐ Constantly

I have reviewed this job description and I understand all my job duties and responsibilities. I am able to perform the essential functions as outlined. If I have any questions about job duties not specified on this description that I am asked to perform, I should discuss them with my manager or a member of the Human Resources team.

I acknowledge that the job has been explained to me both verbally and in written format.

_____ _____

Support Teammate's Signature Date