

# HIPAA Privacy Officer

**Yale University**

Job Location: New Haven, CT

Full Time/Days

## **JOB SUMMARY:**

Reporting to the chief privacy officer, the HIPAA privacy officer is charged with collaboratively developing, implementing, and administering a unified HIPAA Privacy and Security compliance program. The HIPAA privacy officer affects organizational change within the university context of shared governance, mission, and values, and a complex information technology infrastructure and operations.

In collaboration with the chief privacy officer, the HIPAA privacy officer oversees all activities related to the development, implementation, maintenance, and enforcement of the university's policies and procedures covering the privacy of protected health information (PHI). The HIPAA privacy officer directs the deputy privacy officers assigned to the School of Medicine, School of Nursing, Yale Health, Benefits Office, Psychology Department clinics and Human Research Protection Program. The deputy privacy officers have day-to-day responsibility for implementing and enforcing the university's health information policies and procedures within their assigned areas; the HIPAA privacy officer has overarching institutional responsibility for health information privacy and breach notification compliance. The HIPAA privacy officer also supervises a small staff responsible for centralized HIPAA compliance activities. In collaboration with the chief information security officer and the chief privacy officer, the HIPAA privacy officer ensures university security policies and procedures meet HIPAA standards for protecting the confidentiality, integrity and availability of electronic PHI.

## **RESPONSIBILITIES:**

- Develops and implements a comprehensive health information privacy program governing university-wide teaching, research and patient-care operations.
- Manages the HIPAA privacy office staff. Provides oversight and guidance to deputy HIPAA privacy officers and departmental HIPAA contacts to ensure a consistent compliance program across the university.
- In collaboration with the chief privacy officer, develops university-wide policies, procedures and practices governing the privacy and security of health information through the sophisticated analysis of data, operations, and regulatory requirements.
- Promotes a culture of respect for patient privacy and HIPAA compliance in alignment with Yale's teaching, research and patient care missions.
- Directs the identification, implementation, and maintenance of PHI privacy and breach notification policies and procedures in coordination with senior leaders from the university's health care and health plan components, the chief privacy officer, and university attorneys. Assesses, benchmarks, and revises policies and procedures related to appropriate access to PHI in accordance with legal standards and industry best practices.
- Collaborates with strategic partners to assess the security of health-related IT systems, to manage IT-related risk, to ensure regulatory compliance, to align security and privacy practices, and to adapt policies, approaches, and standards to evolving technological challenges.
- Establishes the parameters and standards for ongoing compliance monitoring activities in coordination with the university's other compliance and operational assessment functions.
- Ensures the university's IRBs' compliance with HIPAA privacy policies and procedures.
- Develops and implements a robust privacy and security training and awareness program for diverse university stakeholders, including students, faculty, and medical and professional staff.
- Analyzes university and industry data to identify incident trends related to risks to the privacy of PHI and develops strategies to manage and mitigate those risks.
- Drives HIPAA privacy compliance efforts with affiliated entities and entities participating in an Organized Health Care Arrangement with the university.

- Develops, implements, and monitors business associate agreements to ensure all privacy requirements are addressed.
- Establishes and administers a process for receiving, documenting, tracking, investigating and acting on complaints concerning the university's HIPAA privacy practices, in consultation with the chief privacy officer. Ensures HIPAA investigations are conducted in accordance with university disciplinary policies and are documented in keeping with HIPAA record retention requirements.
- Ensures the consistent application of sanctions for failure to comply with HIPAA privacy policies, in coordination with human resources, the information security officer, the chief privacy officer, and university attorneys.
- Other tasks as assigned.

**REQUIRED EDUCATION AND EXPERIENCE:**

- Bachelor's degree and a minimum of 7 years of experience or equivalent combination of education and experience.

**REQUIRED SKILL/ABILITY:**

- Comprehensive knowledge of (i) health information privacy laws, including HIPAA, HITECH, and OCR guidance; (ii) use of health information in clinical research; and/or (iii) medical records management, including access, release and tracking techniques.
- Ability to work independently and leverage networks to advance programmatic goals in a decentralized environment.
- Ability to promote privacy compliance across a diverse workforce
- Excellent leadership, project management, organizational, and communication skills.

**PREFERRED EDUCATION, EXPERIENCE AND SKILLS:**

- Advanced degree in relevant area such as healthcare, healthcare administration, or law and five years of experience in managing privacy compliance, preferably at an academic medical center, or an equivalent combination of training and experience.

**FOR MORE INFORMATION/TO APPLY:**

[https://sjobs.brassring.com/TGnewUI/Search/Home/Home?partnerid=25053&siteid=5248#jobDetails=1564743\\_5248](https://sjobs.brassring.com/TGnewUI/Search/Home/Home?partnerid=25053&siteid=5248#jobDetails=1564743_5248)