JOB DESCRIPTION TEMPLATE

HIPAA Privacy Officer

The HIPAA Privacy Officer is the designated privacy official required under 45 CFR 164.530, accountable for how protected health information is used, disclosed, and protected.

Employment type Full-time

POSITION OVERVIEW

The Privacy Officer owns how protected health information is used, disclosed, and safeguarded across the organization.

The role is named in law. 45 CFR 164.530 requires a designated privacy official, which makes this one of the few compliance jobs a regulator will ask you to point at by name.

It sits between clinical operations, IT security, legal, and the patients themselves, and it is judged on whether breaches are prevented, found early, and handled correctly.

KEY RESPONSIBILITIES

UNDEFINED

UNDEFINED

UNDEFINED

UNDEFINED

UNDEFINED

UNDEFINED

UNDEFINED

REQUIRED QUALIFICATIONS

- Five or more years in healthcare privacy, health information management, or healthcare compliance.
- Working command of the HIPAA Privacy Rule, Breach Notification Rule, and the interaction with state privacy law, which is often stricter.
- Direct experience running a breach investigation, including the notification decision.
- Experience with 42 CFR Part 2, state health privacy statutes, and consent management.
- Ability to explain a privacy restriction to a frustrated clinician without losing the clinician.
- Bachelor's degree, or equivalent healthcare compliance experience.

PREFERRED CERTIFICATIONS

CHPC, CIPP/US, CHC, RHIA, or CHPS are the credentials that carry weight here.

TECHNICAL KNOWLEDGE

Electronic health record audit tools (Epic, Cerner, Meditech), privacy monitoring platforms, GRC systems, and consent management tooling. Increasingly, the ability to assess AI tools that touch PHI, including ambient scribes and clinical decision support.

ESSENTIAL COMPETENCIES

Judgment under pressure, plain-language communication with clinicians and patients, investigative discipline, and the confidence to stop a data flow that leadership wants to keep.

WHAT GOOD LOOKS LIKE IN YEAR ONE

- Breach response timelines met without exception.

- Business Associate Agreements current and complete across every vendor touching PHI.
- Patient rights requests answered inside statutory deadlines.
- Workforce training completion above target, with sanctions applied consistently.
- Privacy risk analysis refreshed and its findings actually closed.
- Zero repeat findings from the prior year's audits.
- Clinical leaders bring you in before a new tool goes live, not after.
- No OCR corrective action open at year end.
