**JOB DESCRIPTION FOR YOUR OFFICE’S COMPLIANCE, HIPAA, SECURITY AND PRIVACY OFFICER POSITIONS.**

|  |
| --- |
| HIPAA SECURITY OFFICER JOB DESCRIPTION |
| **POSITION OVERVIEW**:  To the best of his or her ability, the HIPAA Security Officer will ensure that the Company will:   1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the Company creates, receives, maintains, or transmits. 2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. 3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule. 4. Ensure compliance with the provisions of the HIPAA Security Rule by the Company’s workforce. |
| **PRIMARY JOB DUTIES AND RESPONSIBILITIES:**  The HIPAA Security Officer shall have the following primary job duties and responsibilities:   1. Serve as an expert and advisor on information management matters within the Company and be responsible for emergency planning and disaster recovery, as well as compliance with applicable State and Federal security rules. 2. Assure that the security standards stipulated as part of the HIPAA Security Rule are adopted and remain current within the Company. 3. Develop and implement policies, procedures, and regulations that include: 4. technological protection for information technology systems containing electronic protected health information, 5. firewall management, 6. internal investigations, 7. crisis management, 8. contingency planning, 9. data backup planning, 10. disaster recovery planning, 11. information access controls, 12. internal controls, 13. internal audits, 14. workstation security, 15. applications and data analysis, 16. hardware and software installation, 17. virus checking, 18. security testing, 19. security incident reporting and response, and 20. access termination processing. 21. Maintain records of access authorizations and review the level of access granted to a user, program or procedure, accessing health information on an on-going basis. 22. Monitor the Company’s compliance with applicable laws and regulations; monitor the Company’s compliance with the information security and HIPAA policies and procedures among employees, business associates, and other third parties. 23. Report security issues to senior management, including the Compliance Officer, the Company’s attorney and the Company’s leadership, where applicable. 24. Monitor internal control systems to ensure that appropriate access and authorization levels and security clearances are maintained. 25. Establish personnel clearance and termination procedures. 26. Assist the Compliance Officer with implementing security training programs for HIPAA and any other appropriate rules or regulations as they apply for the Company; assure that all appropriate personnel are trained and that training records are updated in the compliance data base maintained by the Company’s Compliance Officer, or his or her designee. 27. Assure that the Company has appropriate updated and applicable disaster recovery and business continuity plans for its information technology systems and electronic protected health information storage, communication and data sharing mechanisms. 28. Perform security audits and risk assessments as necessary in accordance with the Company’s information systems audit policies and in a manner that is compliant with the HIPAA Security Rule. 29. Serve as the Company’s Designated Approving Authority and issue an Authorization to Operate (ATO), which is a formal declaration that authorizes operation of the Company’s information systems as they may pertain to certain business products and operation and explicitly accept the risk to the Company’s operations. The ATO is signed after an independent audit certifies that the Company’s information system as they may pertain to certain business products and operation has met and passed certain requirements to become operational. 30. Provide consulting support and make recommendations to the Company’s Compliance Officer, senior management and leadership council, where applicable, regarding appropriate, timely and necessary security improvements, enhancements, or policy interpretations. 31. Monitor legislative and regulatory changes that impact Company-wide security practices, including but not limited to, breach notification, remote access, media destruction, and the use and inherent risks associated with portable computing devices and social media. 32. Coordinate ongoing review of existing security programs and initiate the development of new programs and approaches as needed. 33. Serve as the HIPAA Security information liaison to marketing, product development, administrative and executive staff. 34. Develop metrics to continuously measure security effectiveness within the Company, and continuously monitor and report on the status of those metrics and compliance with the HIPAA Security Rule. 35. Assist the Compliance Officer as necessary with managing the ongoing HIPAA Security Rule compliance program in the Company to assure timely and complete compliance with the applicable standards identified in the law. 36. Periodically report on the status, issues, and risks of the Company’s efforts to the Company’s Compliance Officer, senior management and/or leadership council, where applicable. |
| **MINIMUM QUALIFICATIONS:**   * BA or BS in Computer Science, Information Systems, or Master’s degree in a related field, or equivalent experience; * Experience in the healthcare or financial industry in a senior security role; * 10+ years in information security with progressive experience in the following areas: * Security policy development * Security and Information technology audits * Business and operational risk assessments * Network security architecture * Application and database security * Security infrastructure technologies - Firewalls, Intrusion Detection Systems (IDS) * Expertise in vulnerability analysis; * A comprehensive understanding of the HIPAA Security Rule, the HITECH Act amendments that affect the HIPAA Security Rule, and all other relevant security laws, regulations, and standards that apply to the Company; * Expertise on industry security standards such as NIST, FISMA, ISO 27002 and CobiT 4.1; * Project Management skills and experience; * Technical Writing experience or equivalent; * Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and other certifications preferred; * Demonstrated leadership abilities; * Experience in working with boards of directors, senior executives, department managers, consulting and other counsel; * Training skills and experiences; * Relative comfort in confronting difficult situations, potentially involving the activities of employees and/or other parties; and * Ability to get along with diverse personalities, to be tactful, mature, and flexible. |
| HIPAA Security Rule 45 CFR 164.306(a)(1) (General Requirements) “Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.”  HIPAA Security Rule 45 CFR 164.306(a)(2)(General Requirements) “Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.”  HIPAA Security Rule 45 CFR 164.306(a)(3)(General Requirements) “Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [the Privacy Rule].”  HIPAA Security Rule 45 CFR 164.306(a)(4) (General Requirements) “Ensure compliance with [the Security Rule] by its workforce.”  HIPAA Security Rule 45 CFR 164.308(a)(2)(i)(Assigned Security Responsibility) “Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.” |

|  |
| --- |
| COMPLIANCE OFFICER JOB DESCRIPTION |
| The Compliance Officer is responsible for directing and assuring the active functioning of the Company’s compliance efforts.  As such, the Compliance Officer oversees, coordinates and monitors the day-to-day compliance activities of the Company.  General responsibilities of the Compliance Officer include the following:  Supervising prompt implementation of the Compliance Plan and coordinating all compliance efforts.   1. Ensuring that the Covered Individuals receive a copy of the Compliance Plan, which includes the Code of Conduct and, depending on an individual’s particular job responsibilities, any other written compliance policies and guidelines that may be applicable to their duties. 2. Assisting in developing and approving compliance education and training materials, and documenting and implementing tracking mechanisms to document completion of required training, and overseeing annual attestations by Covered Individuals regarding commitment to compliance. 3. Coordinating compliance personnel issues with the Company’s human resources manager to ensure that compliance is an integral part of performance assessment and that the processes set forth in this Compliance Plan relating to the screening of Covered Individuals are completed. 4. Developing communications (e-mails, newsletters, etc.) that encourage Covered Individuals to report possible compliance issues. 5. Implementing and operating retaliation-free reporting channels, including the Compliance Hotline. 6. Ensuring that vendors who furnish items or services to Sound are aware of this Compliance Plan and, where appropriate, agree to abide by this Compliance Plan. 7. Identifying and assessing areas of the Company operations that present the greatest compliance risk, developing an annual auditing plan to assist in reducing such risks and otherwise prioritizing resources to address such risks. 8. Working with the Ethics & Compliance Committee to identify risk areas warranting compliance audits and other monitoring methods. 9. Monitoring and evaluating the Compliance Plan’s effectiveness through internal and external audits, overseeing internal or external resources conducting compliance audits, and assessing results and developing any necessary responses or corrective actions. 10. Overseeing and documenting any compliance investigations, and working with legal counsel as the situation warrants. 11. Reporting on a regular basis to the Company’s Chief Executive Officer, the Ethics & Compliance Committee and the Company’s leadership regarding day-to-day compliance efforts (which may include, without limitation, a summary of current auditing and monitoring efforts, as well as statistical and trending information) and promptly reporting the results of material or significant investigations. 12. Keeping current with laws, regulations and policies applicable to compliance in order to provide the best possible advice and guidance and reviewing regulations, policies and other guidance released by applicable Federal and State agencies to ensure that the Compliance Plan and other relevant policies addresses the items set forth by such guidance and updating policies as appropriate. 13. Periodically, but at least annually, with the Ethics & Compliance Committee, assessing the adequacy of the Compliance Plan (including, without limitation, the Code of Conduct) and revising as necessary. 14. Responding to potential violations. |
| MINIMUM REQUIREMENTS:   1. Education: A Bachelor’s degree required; Master’s desired; Juris Doctor preferred. 2. Experience: A minimum of 10 years’ experience in a healthcare organization, to include demonstrated leadership. Familiarity with operational, financial, quality assurance, and human resource procedures and regulations is a must. 3. Certifications: Certified in Healthcare Compliance (CHC), Certified Professional Compliance Officer (CPCO) |

|  |
| --- |
| HIPAA PRIVACY OFFICER JOB DESCRIPTION |
| 1. Provides leadership to the Company’s committees, work groups, and task forces charged with creating and implementing a privacy program.  a. Develops Company privacy policies and procedures consistent with applicable laws, rules, and regulations to ensure the protection of individually identifiable health information within the Company.  b. Ensures that privacy requirements are implemented into existing business operations to maintain compliance with Federal and State laws related to privacy, security, confidentiality, and protection of information resources and protected health information.  c. Develops, implements, and administers authorization procedures for access to, use, and disclosure of protected health information.  d. Develops, implements, and administers procedure to allow individuals to exercise their rights to protected health information under applicable State and Federal Laws.  e. Creates, posts, distributes and responds to individual requests for further information concerning the Notices of Privacy Practices.  f. Develops and implements privacy training programs and a security awareness and training program.  g. Ensures applicable privacy training delivery to Company’s staff and extended workforce.  h. Coordinates with Human Resources to develop appropriate sanctions for employees or business partners that fail to comply with the Company’s privacy policies and procedures.  i. Coordinates with the Company’s management to measure the effectiveness, performance, and quality of the company’s privacy program.  j. Escalates privacy issues to the Company’s senior management as appropriate.  k. Monitors state and federal privacy legislation.  l. Leads periodic federal and state Privacy protected health information assessments.  2. Monitors complaints and information relating to Company’s privacy program and investigates all allegations of non-compliance with the Company’s privacy policies.  3. Coordinates with other applicable departments regarding the mitigation of the effects of any unauthorized or otherwise inappropriate release of health information.  4. Reports on the status of the privacy program to Company leadership on a periodic basis. |
| MINIMUM QUALIFICATIONS:   * + - 1. Minimum ten years’ experience in health care, compliance or law. Demonstrated above average professional judgment, communication, reasoning and decision-making skills;       2. Minimum educational requirements: J.D. preferred; master’s degree required;       3. Certified Information Privacy Professional – United States (CIPP/US), Certified HIPAA Professional (CHP) strongly preferred.       4. A comprehensive understanding of the HIPAA Privacy Rule, the HITECH Act amendments that affect the HIPAA Privacy Rule, and all other relevant privacy laws, regulations, and standards that apply to the Company;       5. Demonstrated leadership abilities;       6. Experience in working with boards of directors, senior executives, department managers, consulting and other counsel;       7. Training skills and experiences;       8. Relative comfort in confronting difficult situations, potentially involving the activities of employees and/or other parties; and       9. Ability to get along with diverse personalities, be tactful, mature and flexible. |