

EXHIBIT 1

(Insert Practice Name)

SECURITY OFFICIAL JOB RESPONSIBILITIES

The Security Official for this practice oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures related to the security of patients' electronic protected health information (EPHI) in compliance with federal and state laws and the practice's security policies and procedures (the "Security Policy").

Responsibilities:

- Maintains the confidentiality, integrity, and availability of patients' EPHI.
- Maintain current knowledge of applicable federal and state security laws.
- Develop, oversee, and monitor implementation of the practice's Security Policy and ensure that the integrity of the Security Policies is maintained at all times.
- Report regularly to the practice governing body and officers and/or owners (as applicable) regarding the status of the Security Policies.
- Work with legal counsel, consultants, management, and committees to ensure that the practice maintains appropriate administrative materials in accordance with practice management and legal requirements.
- Establish and administrate a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the practice's security policies and procedures in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.
- Oversee, direct, deliver, or ensure the delivery of security training and orientation to all employees, volunteers, medical and professional staff, and other appropriate personnel (practice workforce).
- Monitor attendance at all Security Policies training sessions and evaluate participants' comprehension of the information provided at training sessions as well as maintain appropriate documentation of security training.
- Monitor practice compliance with Security Policies including periodic security risk assessments.
- Monitor and evaluate, on no less than an annual basis, the Security Policies success in meeting the practice's goal for protection of EPHI.
- Coordinate and participate in disciplinary actions related to the failure of practice workforce members to comply with the practice's Security Policies and/or applicable law.
- Monitor access controls to EPHI. Maintain access to EPHI only by authorized personnel.

- Monitor technological advancements related to electronic protected health information protection and security for consideration of adaptation by the practice.
- Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Security Policies.
- Initiate, facilitate, and promote activities to foster security information awareness within the practice.
- Cooperate with CMS, other legal entities, and practice officers or owners in any compliance reviews or investigations.
- Perform periodic risk assessments and ongoing compliance monitoring activities at each practice location.
- Act as point of contact for the practice's legal counsel in an ongoing manner and in the event of a reported violation.
- Maintain all business associate contracts and respond appropriately if problems arise.
- Act as the practice-based point of contact for receiving, documenting, and tracking all complaints concerning security policies and procedures of the practice.
- Maintain documentation of the practice's Security Policies and Procedures for a minimum of six years from the date the practice created the policies and procedures or last updated the policies and procedures.
- Responsible for overseeing the maintenance of the practice's hardware and software.
- Accountable for tracking hardware and software inventory.
- Responsible for overseeing the installation and connectivity of computer equipment.
- Responsible for monitoring daily, weekly, and monthly backup procedures.
- Responsible for disposal and media re-use.

Skills:

- Able to facilitate change.
- Possess knowledge and understanding of federal and state security laws and of the medical practice's information technology. **[list technology used]**

EXHIBIT 1A

(Insert Practice Name)

PRIVACY & SECURITY OFFICIAL JOB RESPONSIBILITIES

The Privacy & Security Official for this practice oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures related to the privacy and security of patients' protected health information (PHI) in compliance with federal and state laws and the practice's privacy and security policies and procedures.

Responsibilities:

- Maintain the confidentiality, integrity, and availability of patients' PHI.
- Maintain current knowledge of applicable federal and state privacy and security laws.
- Develop, oversee, and monitor implementation of the practice's Privacy and Security Policies and ensure that the integrity of the Privacy and Security Policies is maintained at all times.
- Report regularly to the practice governing body and officers (as applicable) regarding the status of the Privacy and Security Policies.
- Work with legal counsel, management, and committees to ensure that the practice maintains appropriate privacy consent and authorization forms, notices, and other administrative materials in accordance with practice management and legal requirements.
- Establish and administrate a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the practice's privacy and security policies and procedures in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.
- Establish and oversee practice policies for addressing patient requests to obtain or amend patient records, restrict the means of communication, or obtain accountings of disclosures; ensure compliance with practice policies and legal requirements regarding such requests and establish and oversee grievance and appeals processes for denials of requests related to patient access or amendments.
- Oversee, direct, deliver, or ensure the delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, and other appropriate personnel (practice workforce) and maintain appropriate documentation of privacy training.
- Monitor attendance at all Privacy and Security Policies training sessions and evaluate participants' comprehension of the information provided at training sessions.
- Monitor compliance with Privacy and Security Policies including periodic privacy risk assessments.
- Monitor and evaluate, on no less than an annual basis, the Privacy and Security Policies' success in meeting the practice's goal for protection of PHI.
- Coordinate and participate in disciplinary actions related to the failure of practice workforce members to comply with the practice's Privacy and Security Policies and/or applicable law.
- Monitor access controls to EPHI. Maintain access to EPHI only by authorized personnel.
- Monitor technological advancements related to protected health information protection and privacy for consideration of adaptation by the practice.

- Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Privacy and Security Policies.
- Initiate, facilitate, and promote activities to foster privacy and security information awareness within the practice.
- Cooperate with the Office of Civil Rights, CMS, other legal entities, and practice officers or owners in any compliance reviews or investigations.
- Perform periodic risk assessments and ongoing compliance monitoring activities at each practice location.
- Act as point of contact for practice's legal counsel in an ongoing manner and in the event of a reported violation.
- Maintain all business associate contracts and respond appropriately if problems arise.
- Act as the practice-based point of contact for receiving, documenting, and tracking all complaints concerning privacy and security policies and procedures of the practice.
- Maintain documentation of the practice's security policies and procedures for a minimum of six years from the date the practice created the policies and procedures or last updated the policies and procedures.
- Responsible for overseeing the maintenance of the practice's hardware and software.
- Accountable for tracking hardware and software inventory.
- Responsible for overseeing the installation and connectivity of computer equipment.
- Responsible for monitoring daily, weekly, and monthly backup procedures.
- Responsible for disposal and media re-use.

Skills:

- Able to facilitate change.
- Possess knowledge and understanding of federal and state privacy security laws of the medical practice's information technology. **[list technology used]**