**HIPAA Security Program Policy and Procedures for Security Officer**

### Purpose:

### To comply with the Administrative Safeguards of HIPAA Security, to secure and maintain the confidentiality of Protected Health Information, maintain sensitive organizational information at [Insert Covered Entity Name] and prevent and detect inappropriate and illegal uses and disclosures.

### Policy:

### [Insert Covered Entity Name] shall be responsible for implementation of the administrative requirements under the Federal HIPAA Security Rule.

### [Insert Covered Entity Name] will designate a privacy official to be responsible for the development and implementation of the policies and procedures of [Insert Covered Entity Name].

1. **Definitions:**
	1. HIPAA: Health Insurance Portability and Accountability Act of 1996.
	2. Individually Identifiable Health Information (IIHI): Under Section 160.103 of HIPAA, IIHI is defined as information that is a subset of health information, including demographic information collected from an individual, and:
		1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse.
		2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
		3. That identifies the individual.
		4. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
		5. IIHI includes identifiers of the patient, relatives, employers, or household members such as the following (§164.514):
			1. Names.
			2. Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code (except for the initial 3 digits of a zip code if, according to the current publicly available data from the Bureaus of the Census all zip codes with the same 3 initial digits contains more than 20,000 people).
			3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
			4. Telephone numbers.
			5. Fax numbers.
			6. Email addresses.
			7. Social security numbers.
			8. Medical record numbers.
			9. Health plan beneficiary numbers.
			10. Account numbers.
			11. Certificate/license numbers.
			12. Vehicle identifiers and serial numbers, including license plate numbers.
			13. Device identifiers and serial numbers.
			14. Biometric identifiers, including finger and voice prints.
			15. Full face photographic images and any comparable images.
			16. Any other unique identifying number, characteristic, or code.
	3. Protected Health Information (PHI): Under Section 164.501 of HIPAA, PHI means IIHI that is transmitted and maintained in electronic media or in any other form or medium.
	4. Designated Record Set: In compliance with §164.524 contained within the Privacy Rule of the Administrative Simplification provisions of HIPAA, [Insert Covered Entity Name] maintains a designated record set (DRS). The designated record set includes medical and billing records that patients and/or their personal representatives have the right to access, inspect, and copy. Records include any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a provider (§164.501).
	5. Provider: Under Section 160.103 of HIPAA, a provider of medical or health services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u) and 1861(s) of the Act, 42 U.S.C. 1395x(s)) and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Providers are those contracted, subcontracted, or employed by [Insert Covered Entity Name] who provide services on behalf of [Insert Covered Entity Name].
2. **Procedures**
	1. [Insert Covered Entity Name] is committed to complying with the HIPAA Security Rule and maintaining the confidentiality of patients’ PHI through appropriate, authorized access, uses, and disclosures.
	2. [Insert Covered Entity Name] and its business affiliates create, store, maintain, use, transmit, collect and disseminate PHI in an environment that promotes confidentiality and integrity without compromising PHI.
	3. Confidentiality policies and procedures are reinforced throughout [Insert Covered Entity Name] and followed by all physicians, employees, and business associates.
	4. The [HIPAA Security Officer or Office Manager] oversees the HIPAA Security program.
	5. The [HIPAA Security Officer or Office Manager] is responsible for the following functions, which support compliance with the HIPAA Security Rule, patient confidentiality, access laws and [Insert Covered Entity Name] policies and procedures pertaining to them:
		1. Maintain current and appropriate body of knowledge necessary to perform the Security Officer function.
		2. Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information security technologies to ensure organizational adaptation and compliance.
		3. Maintain working knowledge of legislative and regulatory initiatives. Interpret and translate requirements for implementation.
		4. Work effectively with the Privacy Officer, other information security personnel and the committee process.
		5. Monitor Information Security Program compliance and effectiveness in coordination with the [Insert Covered Entity Name] other compliance and operational assessment functions.
		6. Oversee, direct, deliver, or ensure delivery of security training and orientation to all employees.
			1. To each employee by no later than the compliance date for [Insert Covered Entity Name].
			2. To new employees during their first month of employment.
			3. To existing employees annually.
			4. To existing employees whose functions are affected by a change in the policies and procedures, within a month after the change comes into effect.
		7. Establish a mechanism to track access to PHI, within the purview of [Insert Covered Entity Name] and as required by law and to allow qualified individuals to review or receive a report on such activity.
		8. Initiate, facilitate and promote activities to foster information security awareness within the organization and related entities.
			1. Send out regular security tip emails to all employees.
			2. Create regular security workshops.
			3. Utilize games to roll out security tips, but to make it more engaging.
		9. Maintain a program encouraging employees and patients to report complaints concerning compliance of the law and [Insert Covered Entity Name] policies and procedures to [HIPAA Security Officer or Office Manager].
		10. Conduct investigations of information security violations and computer crime. Work with management and external law enforcement to resolve these instances.
		11. Document all complaints and investigations into security violations [§164.530(d)(2)].
		12. Ensure compliance with security practices and consistent application of sanctions for failure to comply with security policies for all of the [Insert Covered Entity Name] employees and for all business associates, in cooperation with Human Resources, the Privacy Officer, administration, and legal counsel as applicable.
		13. Document actions taken against employees who failed to comply with the policies and procedures [§164.530(e)(2)].
		14. Mitigate, to the extent practicable, any harmful effect that is known to the [Insert Covered Entity Name] of a security violation [§164.530(f)].
		15. Serve as information security consultant to the organization for all departments and appropriate entities.
		16. Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
		17. Determine positions and personnel necessary to accomplish information security goals.
		18. Grant and remove access to ePHI systems, as necessary.
			1. Ensure that only employees who require access to ePHI are granted access.
			2. Screen employees prior to granting access.
			3. Before granting access in any of the various systems or applications that contain ePHI, employees shall be trained to include:
				1. Proper uses and disclosures of the EPHI stored in the systems or application.
				2. How to properly log on and log off the systems or application.
				3. Protocols for correcting user errors.
				4. Instructions on contacting a designated person or help desk when ePHI may have been altered or destroyed in error.
				5. Reporting a potential or actual security breach.
			4. Require employees being issued a User ID or logon account for accessing any ePHI to sign the Acknowledgement of Information Security Responsibility before access is granted to the network or any application that contains ePHI.
				1. All requests regarding User IDs or computer system access for employees are to be communicated to the appropriate system administrator by completing the required form(s) for covered components. All requests shall be made in writing (which may be in an electronic format).
			5. The [HIPAA Security Officer or Office Manager] has the authority to grant emergency access for employees who have not completed the normal HIPAA access requirements if:
				1. The facility declares an emergency or is responding to a natural disaster that makes the management of client information security secondary to immediate personnel safety activities.
				2. Management determines that granting immediate access is in the best interest of the client.
			6. If [HIPAA Security Officer or Office Manager] grants emergency access, she/he shall review the impact of emergency access and document the event within 24 hours of it being granted.
			7. After the emergency event is over, the user access shall be removed or the employee shall complete the normal requirements for being granted access.
			8. In some circumstances it may be necessary for management to grant emergency access to a user’s account without the user’s knowledge or permission. [HIPAA Security Officer or Office Manager] may grant this emergency access in these situations:
				1. The workforce member terminates or resigns and management requires access to the person’s data.
				2. The workforce member is out for a prolonged period.
				3. The workforce member has not been in attendance and therefore is assumed to have resigned.
				4. Manager/supervisor needs immediate access to data on a workforce member’s computer in order to provide client treatment.
		19. The [HIPAA Security Officer or Office Manager] or his/her designated representative is responsible for terminating an employee’s access to ePHI in these circumstances:
			1. If management has evidence or reason to believe that the individual is using information systems or resources in a manner inconsistent with the Security Rule policies.
			2. If the employee or management has evidence or reason to believe the user’s password has been compromised.
			3. If the employee resigns, is terminated, is suspended, retires, or is away on unapproved leave.
			4. If the employee’s job description changes and system access is no longer justified by the new job description.
			5. If the employee is on an approved leave of absence and the user’s system access will not be required for more than three weeks, [HIPAA Security Officer or Office Manager] shall suspend the user’s account until the employee returns from their leave of absence.
		20. If an employee transfers to another program or changes roles within the same program within the [Insert Covered Entity Name] covered component:
			1. The employee’s new supervisor or manager or [HIPAA Security Officer or Office Manager] is responsible for evaluating the employee’s current access and for requesting new access to ePHI commensurate with the employee’s new role and responsibilities.
		21. In order to ensure that employees only have access to ePHI when it is required for their job function, the following actions shall be implemented by all covered components:
			1. Every new User ID or log on account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the employees still requires access to the ePHI.
			2. Supervisors/managers (or appropriate designees) must maintain:
				1. A list of all employees for all applications
				2. A list of employees and their access rights for all shared folders that contain ePHI
				3. A list of all Virtual Private Network employees
				4. The supervisors/managers shall notify [HIPAA Security Officer or Office Manager] of any employees that no longer require access.
3. **Documentation:**
	1. All documentation related to and/or required by HIPAA, including but not limited to compliance enforcement, activities such as training, policies and procedures, complaint investigations, designated record sets, etc. are maintained for six years from the date of creation, or the date it was last in effect, whichever is later [§164.530(j)]. Documentation may be maintained in written or electronic form [§164.530(j)(1)(ii)].