Many states have consumer or patient privacy laws that are more stringent than HIPAA. For example, while HIPAA has clear regulations for the disposal of protected health information kept in electronic formats, it does not have clear regulations for destruction of paper records. We make this sample policies and procedures available to our physician clients to help them become aware of privacy compliance obligations beyond HIPAA. Please be advised that this guide is **only a sample**, so be sure to consult with your attorney to ensure that the final policy you adopt is compliant with the laws of your state.

*Instructions: Read through the sample and choose the best policy for your practice. Fields highlighted in green indicate where edits or policy choices need to be made.*

SAMPLE POLICIES AND PROCEDURES FOR

MANAGEMENT OF PERSONAL PROTECTED INFORMATION

(*Effective [Date], Revised [Date]*)

1. For purposes of this policy & procedures, Protected Information (“PI”) includes, but may not be limited to: [Select all that apply.]
* Biometric Data
* Driver’s License Numbers
* Employer, Student, or Military Identification Numbers
* Financial Account Numbers or other Financial Transaction Devices
* Government Issued Identification Card Numbers
* Other:
* Pass Codes
* Passport Numbers
* Passwords
* Personal Identification Numbers
* Social Security Numbers
1. Our office maintains PI in the following formats: [Select all that apply.]
* Paper records
* Electronic records
* Other digital formats such as:
* Other:
1. Our office policy is to take reasonable security measures to protect PI. [Decide whether you prefer to (1) outsource security or (2) provide your own security; pick one option based on the size and nature of your business. If you choose to provide your own security, choose one of the options indicated in that field.]
* Based on the size and nature of our business, we elect to engage the following third-party service provider: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Our office requires that this provider shall ensure that it implements and maintains reasonable security procedures and practices that are (1) appropriate to the nature of the PI; and (2) reasonably designed to help protect the PI from unauthorized access, use, modification, disclosure, or destruction.

***ALTERNATIVELY***

* Based on the size and nature of our business, we elect to provide our own PI security protection including technical controls that are reasonably designed to enact the following security measures in our office:
* help protect the PI from unauthorized access, use, modification, disclosure, or destruction; ***OR***
* effectively eliminate the ability of a third-party to access the PI, notwithstanding the third-party’s physical possession of the PI.

These technical controls include, but may not be limited to, the following: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. It is the policy of our office to destroy or otherwise dispose of PI when it is no longer needed. PI is determined to be no longer needed when: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Upon determination that disposal is appropriate, the procedure to effectuate this policy is as follows:
	1. Paper records are to be: [Select all that apply.]
* Shredded in office
* Destroyed by a recycler or disposal firm contractually obligated to verify that the PI has been properly destroyed or disposed of commensurate with state law.
	1. Electronic records are to be: [Select all that apply.]
* Erased
* Modified such that PI is de-identified
* Otherwise rendered unreadable or undecipherable through any means.
1. Our office is under the jurisdiction of the State of \_\_\_\_\_. State law [Select one based on the laws of your state.]
* DOES; or
* DOES NOT

require notification in the event of a security breach.

1. Security Breach Procedures:
	1. If our office becomes aware that a security breach may have occurred, we will conduct a good-faith investigation to determine the likelihood that PI has been, or will be, misused.
	2. If our investigation determines that misuse has not occurred, and is not reasonably likely to occur, then no notice shall be given.
	3. If our investigation determines that misuse has occurred, or is reasonably likely to occur, then we will:
		1. Give notice to the affected person within 30 days of the date of determination of security breach; and
		2. Direct that person to promptly take appropriate steps to protect the affected online account, email address, password, security question(s) and answer(s), login-credentials, etc.
	4. If 500 or more people require notification, then our office will give notice to the Attorney General within 30 days of the date of determination of security breach.
	5. If more than 1,000 people require notification, then our office will expediently notify the consumer reporting agencies of the anticipated number of people that will be notified, and the anticipated date of the notification.
2. No Conflict of Laws: This policy and these procedures are intended to augment, but in no way limit, our obligations under the Health Insurance Portability and Accountability Act and the regulations promulgated thereunder (HIPAA). If there is a conflict between state law and HIPAA as to the notice period, the law or regulation with the shortest timeframe for notice to the individual shall control.

Adopted by: [Name of Privacy Officer]

For: [Name of Practice]

Date: [Date]