Disclaimer, Terms of Use, and Copyrights

The following document is developed by Person-Centered Tech, LLC and is offered for educational purposes. It is not offered with any intent or implied warranty of fitness for a particular purpose nor is there any warranty, guarantee, or general claim that this will in any way provide any particular level of legal protection.

This document is not a substitute for legal advice or consultation, nor is it a substitute for clinical or ethical consultation or advice. State laws and licensing board rules vary, as do the needs of individual clients. You must modify this document – or rules out its use – as necessary according to your local laws and rules as well as the needs of your clients and your practice.

Unless otherwise prohibited by law, Person-Centered Tech, LLC will not be liable to you or to any other third party for: (a) any direct, indirect, incidental, special, punitive, or consequential losses or damages, including, but not limited to, loss of profits, loss of earnings, loss of business opportunities, or personal injuries resulting directly or indirectly from use of this document; or (b) any losses, claims, damages, expenses, liabilities, or costs (including legal fees) resulting directly or indirectly from use of this document. The conditions in this paragraph apply to any acts, omissions, and negligence of Person-Centered Tech, LLC that would give rise to a course of legal action. You agree to indemnify and hold harmless Person-Centered Tech, LLC against all claims and expenses (including attorney fees) arising from the use of this document.

This document is provided “as is.” Person-Centered Tech, LLC grants you right to use this document in your own health care practice. Your right to use this document is non-exclusive and may not be transferred to others. You may copy or modify this document according to your individual business needs, but you may not distribute copies of this document nor may you distribute documents derived from this one. You are also prohibited from using this document for educational purposes without prior written consent.

Using This Document

This document is meant to follow a Risk Analysis and Risk Management planning process. As you'll see below, the documentation for the Risk Analysis and Risk Management plan are meant to be created separately from this document. Those processes, as well as the creation of policies outlined here, are required by HIPAA for compliance.

Risk Analysis and Risk Management?

Risk Analysis and Risk Management are a process by which one identifies risks to protected health information, prioritizes them, and then makes a plan for managing them.

For more information: http://www.youtube.com/watch?v=JllYcEeBZtw

For guidance from the federal government:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

Person-Centered Tech also provides Risk Analysis and Risk Management consultation services for small practices. For details: http://www.personcenteredtech.com/web-consulting-services-and-fees/consulting-for-mental-health-professionals/

General Security Policies

Name or Other Identifier for Covered Entity:
Effective Date:
Designated Security Officer:
Designated Privacy Officer:

Security Management Process

Risk Analysis

See attached documentation

Risk Management Plan

See attached documentation

Sanction Policy:

This is your policy for sanctions you use when an employee breaks one or more of your security and privacy policies. Here we also give space for sanctions against contracted helpers or others close to your practice who have been trained on your policies and break one or more of them. Sanctions can include write-ups, termination of employment, termination of rights to access your assets, etc.

O This covered entity has no employees, contracted helpers or other helpers
O Policy is as follows:

Information System Activity Review Policy:

This policy describes your procedures for how you regularly audit your information systems (computers, online record systems, etc.) for suspicious activities, activities that violate your policies, or signs that security breaches have occurred or were attempted. For many solo practitioners, the needed expertise to perform these reviews is outside of their capabilities. However, some systems provide information that can be used to perform such a review. For example, most online EHR or practice management systems will provide a list of attempts to access the system. Some secure texting apps provide this feature, as well. The firewall on your computer may also have logs that show attempts to access your computer from the Internet or attempts by software on your computer to access the Internet. Your policy may include reviewing these items yourself, hiring an IT expert to review them periodically, or other such procedures.

Policy:

Workforce Security

Authorization and/or Supervision Policy

Here you talk about your policy for determining which of the people working for you or helping you have access to your PHI and which PHI they have access to, as well as how they will be supervised while they are accessing PHI.

O This covered entity has no employees, contracted helpers or other helpers
O Policy is as follows:

Workforce Clearance Procedure

Here you talk about your policy for how you determine if it is appropriate for a given employee or helper to have access to PHI.

O This covered entity has no employees, contracted helpers or other helpers
O Policy is as follows:

Termination Procedure Policy

Here you talk about how you go about terminating access to PHI for employees or helpers who have left your employ. This would include things like changing passwords, deleting user accounts, etc.

O This covered entity has no employees, contracted helpers or other helpers
O Policy is as follows:

Information Access Management

Access Authorization

*Here describe your policies **and procedures** for providing access to PHI to employees and helpers. This would include how your provide access to devices or accounts that contain, create, or transmit PHI. Also include here your procedure(s) for documenting the accesses you have granted. You may have determined these asset-by-asset.*

O This covered entity has no employees, contracted helpers or other helpers
O All access authorization policies and procedures are defined in the respective asset-specific documentation
O Some access authorization policies and procedures are defined in the respective asset-specific documentation
O Policies are as follows:

Access Establishment and Modification

Here describe your policies and procedures for reviewing the access to PHI that employees and helpers have been granted and how you go about changing their access to PHI as you deem necessary or appropriate.

O This covered entity has no employees, contracted helpers or other helpers
O All access establishment and modification policies and procedures are defined in the respective asset-specific documentation
O Some access establishment and modification policies and procedures are defined in the respective asset-specific documentation
O Policies are as follows:

Security Awareness and Training

These policies and procedures are aimed at proactively helping one's workforce keep up with security policies. However, some of this section is directly relevant to the clinician, as well, and may be necessary even if there are no employees or helpers.

Security Reminders

Here talk about how you enact reminders of your security policies for employees and helpers.

O This covered entity has no employees, contracted helpers or other helpers
O Policies and procedures are as follows:

Protection From Malicious Software

*Here describe policies and procedures for protecting PHI from "malicious software," which is also called "malware" at times and includes viruses, worms, trojans, malware introduced when someone downloads or otherwise installs software containing said malware, etc. This policy/procedure is included here because infection by malicious software is most often the result of misuse by people – both you and employees. So your strategy for preventing such infections includes both this behavior-oriented policy that defines how you and your helpers are required to use computers in safe ways in addition to the technical security measure you take of installing anti-virus software and firewalls. Here, describe your policies for how employees, helpers, and **you** are required to make safe use of computers and other assets to prevent infection by malware. These policies often include things like not allowing helpers to install*

software without specific permission or supervision, requiring that software and other files downloaded from the Internet must be scanned for viruses (note that Gmail and some other email programs scan email attachments for viruses automatically), devices may not be allowed to connect to unsecured WiFi networks, etc. Some of your relevant policies and procedures may already be included in your risk management plans related to specific assets. If so, please note that here.

O Policies and procedures are as follows:

Log-In Monitoring

Here is your policy and procedure for monitoring logins by employees and helpers and spotting discrepancies from your policies. This one is a bit redundant with the Information System Activity Review policy. You can reiterate relevant portions of that policy here.

O This covered entity has no employees, contracted helpers or other helpers
O Policies and procedures are as follows:

Password Management

Here you describe policies for creating, changing, and protecting passwords. This is for both you and your employees and helpers. Don't forget that good password habits include changing them regularly. Also, your mobile devices will likely need to be set to allow longer passwords than the default passwords. This set of policies would also cover alternative authentication methods such as thumbprint scans, two-factor authentication, etc.

O Policies and procedures are as follows:

Security Incident Procedures

Here is where you describe your policies or procedures for what to do if a security "incident" occurs. You may have addressed this requirement entirely in your asset-specific risk management plans. E.g. your policy for tracking lost smartphones and tablets would fall under this category. General procedures, such as employing a lawyer and/or IT specialist to help handle security incidents, would be noted here. These things are all specifically mentioned by the HIPAA folks as examples of "security incidents": stolen passwords, corrupted backups, computer viruses, lost or stolen equipment, providing access to PHI to someone who isn't authorized to access. Lost or stolen mobile devices would also be covered here.

O All policies and procedures are defined in the respective asset-specific documentation
O Some policies and procedures are defined in the respective asset-specific documentation
O Policies are as follows:

Contingency Plan

Data Backup Plan

Here is where you would describe how you keep backups of electronic PHI. You may have already covered some or all of this policy in your asset-specific risk management plans.

O All policies and procedures are defined in the respective asset-specific documentation
O Some policies and procedures are defined in the respective asset-specific documentation
O Policies are as follows:

Disaster Recovery Plan

Here is where you describe procedures for restoring lost electronic PHI. Basically, this is where you describe your procedure for restoring PHI from backups. For most folks, this is not a complicated procedure.

O All policies and procedures are defined in the respective asset-specific documentation
O Some policies and procedures are defined in the respective asset-specific documentation
O Policies are as follows:

Emergency Mode Operation Plan

Here you describe procedures for keeping up the security of your PHI when in "emergency mode." "Emergency mode" is not well-defined, but largely includes things like catastrophic loss of power, natural disasters, etc. Here the focus is on how you keep your PHI secure in these situations, which includes how you make sure the data is kept undamaged, confidentiality is ensured, etc. For many of us, the most difficult issue here is how to maintain the accessibility of PHI in these situations. For example, if a power failure results in no Internet connection and all your files are in a cloud-based record system, how do you make sure you can access those files if the necessity arises? This procedure and policy need not be perfect. There will be certain kinds of emergencies for which you may not be able to do much.

O Policies are as follows:

Testing and Revision Procedure

Here you describe procedures for testing your contingency plans periodically to make sure they work and revising them when necessary. For small practices, these procedures need not be overwrought. Remember that simply testing your backups to make sure they actually contain all the information they should and otherwise trying out your other written contingency plans on occasion is sufficient. You simply need to define a plan for doing so.

O Policies are as follows:

Applications and Data Criticality Analysis

This one is not so much a policy or procedure as an analysis. This is where you rank the criticality of your different assets based on what PHI they handle. You do this so you can prioritize which assets are most important to protect and support in an emergency. E.g. if you keep client records primarily on your laptop, then your laptop is likely item number 1. Your phone may be the primary place you keep client contact information, in which case it could also be highly ranked.

1. …
2. …

…

Evaluation

Here, address the requirement that you periodically review all this work you just did to address changes in your environment, tech, etc. You'll want to define how frequently you repeat the whole risk analysis and policy & procedure creation process as well as under what circumstances you'll perform a partial analysis in response to changes. HIPAA does not define how frequently you must repeat the full formal process, but experts generally advise it be done every year. It is inadvisable to repeat this process less than every three years. You may also need to repeat portions of this process if you acquire new assets that handle PHI, modify your existing assets, move offices or add a new office location, etc. Design a policy for how you will evaluate the need to re-evaluate this process and describe it here.

We will repeat the full risk analysis and risk management plan and review security and privacy policies and procedures on the following time schedule:

We will perform a partial analysis and/or review the current analysis and polices & procedures for continuing relevance under the following circumstances:

Business Associate Contracts and Other Arrangements

Generally, Business Associate contracts are addressed in the asset-specific documentation. However, if you wish to describe any further policies or procedures around Business Associates, describe them here.