# Disclaimer, Terms of Use, and Copyrights

The following document is developed by Person Centered Tech Incorporated 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 rule 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 Incorporated 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 Incorporated that would give rise to a course of legal action. You agree to indemnify and hold harmless Person Centered Tech Incorporated against all claims and expenses (including attorney fees) arising from the use of this document.

This document is provided “as is.” Person Centered Tech Incorporated 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.

Your use of this document is also covered by Person Centered Tech’s [Terms of Service](https://personcenteredtech.com/terms-of-service/).

This document is © 2021 Person Centered Tech Incorporated.

Using This Template

This template is for making an agreement between your practice and any companies whose staff members you give an account on any of your systems.

**Example 1**: You work with a virtual assistant (VA) company. You realize that in order for their VA to help you with tasks like managing new client inquiries, you need to give that VA an account in your practice’s email system. Use this template to make an agreement between your practice and the VA service regarding the service’s responsibilities, and those of its designated staff member, vis-a-vis the security of the email account assigned to their staff member.

**Example 2**: Your practice works with a biller who has their own billing service (i.e. they aren’t a workforce member of your practice, and thus they are not directly subject to your policies and procedures.) You realize that for the biller to do their job, they need an account in your practice management system. This will let them directly access information about services provided to clients and do your billing efficiently. Use this template to make an agreement between your practice and the biller’s company regarding the biller’s responsibilities vis-a-vis the security of the practice management system account assigned to their staff member.

Note that this agreement template is not intended to replace or supersede a HIPAA-compliant Business Associate Agreement. This agreement template is intended to set additional expectations over and beyond those of the BAA you execute with these third-party service providers.

**Counterexample:** Your practice management system provides billing services as part of the practice management system service package. The billers at this company can access your client info deeply enough to perform effective billing services. You do not need to make any additional user accounts for them to do so -- the practice management system service manages their access as part of the service you hired them to do. In such a case, you likely will not need to use this agreement template. The BAA and other agreements you entered into with the practice management system are likely to cover the needs that this agreement template addresses.

System Credentials Held By Third Party Secure Use Agreement

This agreement is made between \_\_\_\_\_\_\_\_\_\_\_\_ (“Practice”) and \_\_\_\_\_\_\_\_\_\_\_\_\_ (“Vendor”) on \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Practice and Vendor have jointly determined that, in order to provide necessary services to Practice, one or more of Vendor’s staff members require access credentials for one or more information systems (“Systems”) owned and operated by Practice. Vendor agrees to ensure it implements all security and privacy practices necessary to achieve the following security outcomes (“The Goals”).

# The Goals

* Protect the confidentiality, integrity, and availability of all information held in Systems.
* Prevent unauthorized use or misuse of information held in Systems.
* Ensure that access to Systems via credentials provided by Practice is limited to Vendor’s actively employed staff members who have been assigned those credentials.

This means the Vendor both manages their internal use of the provided credentials according to this agreement, and that Vendor takes all necessary steps to prevent unauthorized access to -- or by way of -- accounts on the Systems which were created for use by Vendor’s staff members.

# Systems and Staff Members

The following staff members at Vendor shall be granted access credentials for the following systems. Credentials and/or access may be revoked by Practice at any time without notice.

| **Staff Member Name** | **System(s) Granted Credentials For** |
| --- | --- |
|  |  |

# Minimum Required Practices

Vendor and it’s staff members agree to implement at least the following security and privacy practices, in addition to any other practices, necessary to achieve The Goals.

1. Passwords and other authentication practices
   1. Passwords used to access Systems are **strong** and **globally unique**. They score as strong when tested by any reasonably acceptable password strength checker. They are not used on more than one system at all, ever, including Practice’s Systems.
   2. Passwords, and any other authentication secrets which may be used, are **never revealed** to anyone, regardless of their position or stated need for the password information.
      1. Vendor ensures that staff who are given access to Systems are trained to detect and resist phishing attacks and other acts of social engineering.
   3. Where Systems make **multi-factor authentication** (MFA) available, Vendor and their staff use it and never deactivate it.
2. Data in Systems is never **forwarded** or **reshared** without specific permission from Practice’s Security Officer**.**
   1. Example 1: email and other messages accessed through Systems are never forwarded outside of Systems without specific permission from Practice’s Security Officer. Sub-example: while Vendor staff members may wish to forward their Practice email to a personally-used email account, doing so would violate this agreement.
   2. Example 2: Systems may offer the ability to share files or other data with outside parties for ease of access. Without specific permission from Practice’s Security Officer, doing so would be a violation of this agreement.
   3. Example 3: Vendor’s staff members never save information from Systems onto their own hard drives or into their own online storage systems, unless Practice’s Security Officer permits or requests it.
3. All devices used to access Systems are **hardened**, and always use a **trusted, secure network connection** when connected to the Internet and other electronic networks.
   1. All devices used to access Systems, regardless of when, why, or how they are used to access Systems, have the following technical security measures in place: full-device encryption; strong passwords for accessing the device; antivirus and/or antimalware software or an equivalent measure (such as on iOS devices and Chromebooks); protection from a firewall or an equivalent measure (such as on iOS devices and Chromebooks).
   2. All devices used to access Systems, regardless of when, why, or how they are used to access Systems, are connected *solely* to networks which are controlled and secured by Vendor according to network security best practices. As an alternative, such devices may connect to other networks if all of the device’s network connections are controlled by VPN software which has a “deadman switch” active.
4. Systems are never used for purposes other than providing services requested by Practice.
5. Vendor will inform Practice immediately when any Vendor staff member, who has been granted access to any Systems, is going to leave Vendor’s employ or has been removed from Vendor’s employ. It is essential that this information be timely, especially if the staff member’s employment is terminated involuntarily.
6. Vendor’s staff members comply with all instruction from Practice’s Security Officer or their representative with regards to access or use of Systems.

## Special Security Practices

<note any special security needs or arrangements here. For example, if you want the Vendor’s staff to use file sharing within your Google account for some specific purpose, specify that here.>

# Remedies for Failure to Achieve the Goals

Vendor agrees to provide the following remedies, where applicable, if Vendor fails to meet the terms of this agreement or specifically violates any of its terms.

* Vendor will pay for all legally-required notification costs, legal fees, consulting fees, and legal penalties in the case of a breach of security or privacy resulting from Vendor’s failure to achieve the Goals.
* Vendor will pay all fees for all services required to repair security or privacy vulnerabilities resulting from Vendor’s failure to achieve the Goals. This includes employment costs for time spent by Practice staff members to repair such vulnerabilities.
* <note any additional remedies you see as necessary or useful for this vendor relationship. Remember that if you also have a Business Associate Agreement with this vendor, that agreement already provides some requirements and potential penalties should the vendor fail to maintain the security and privacy of your PHI. It’s probably not necessary to repeat anything here which is already in the BAA.>

# Approval

By signing below, all approvers agree to all the terms and conditions of this agreement:

| **Practice** | |
| --- | --- |
| Practice Representative (print): |  |
| Signature of Practice Representative: |  |
| Date: |  |
| **Vendor** | |
| Vendor Representative (print): |  |
| Signature of Vendor Representative: |  |
| Date: |  |