CATALYST
COUNSELING

HIPAA AND WASHINGTON STATE NOTICE OF RIGHTS AND PRIVACY PRACTICES

NOTICE:

I keep a record of the health care services I provide you. You may ask me to see and copy that record. You may also ask me to correct that record. I will not disclose your record to others unless you direct me to do so or unless the law authorizes or compels me to do so. You may see your record or get more information about it at Catalyst Counseling, 17330 135th Ave NE, Suite 2B, Woodinville WA 98072.

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Your health record contains personal information about you and your health. State and Federal law protects the confidentiality of this information. Protected Health Information (PHI) is information about you, including demographic information, that may identify you and that relates to your past, present, or future physical and mental health, or condition, and related health care services. If you suspect a violation of these legal protections, you may file a report to the appropriate authorities in accordance with Federal and State regulations.

I am required by law to maintain the privacy of your PHI and to provide you with notice of my legal duties and privacy practices with respect to your PHI. This Notice of Privacy Practices describes how I may use and disclose your PHI in accordance with all applicable law. It also describes your rights regarding how you may gain access to and control your PHI. I am required by law to maintain the privacy of PHI and to provide you with notice of my legal duties and privacy practices with respect to PHI. I am required to abide by the terms of this Notice of Privacy Practices. I reserve the right to change the terms of my Notice of Privacy Practices at any time. Any new Notice of Privacy Practices will be effective for all PHI that I maintain at that time. I will make available a revised Notice of Privacy Practices by sending you an electronic copy, sending a copy to you in the mail upon your request, or providing one to you in person.

How I am permitted to Use and Disclose Your PHI

For Treatment. I may use medical and clinical information about you to provide you with treatment services.
For Payment. I may use and disclose medical information about you so that I can receive payment for the treatment services provided to you.
For Healthcare Operations. I may use and disclose your protected PHI for certain purposes in connection with the operation of my professional practice, including supervision and consultation.
Without Your Authorization. State and Federal law also permits me to disclose information about you without your authorization in a limited number of situations, such as with a court order.
With Authorization. I must obtain written authorization from you for other uses and disclosures of your PHI. You may revoke such authorizations in writing in accordance with 45 CFR. 164.508(b)(5).
Incidental Use and Disclosure. I am not required to eliminate every risk of an incidental use or disclosure of your PHI. Specifically, a use or disclosure of your PHI that occurs as a result of, or incident to an otherwise permitted use or disclosure is permitted as long as I have adopted reasonable safeguards to protect your PHI, and the information being shared was limited to the minimum necessary.

Examples of How I May Use and Disclose Your PHI

Listed below are examples of the uses and disclosures that I may make of your PHI. These examples are not meant to be a complete list of all possible disclosures, rather, they are illustrative of the types of uses and disclosures that may be made.

Treatment. Your PHI may be used and disclosed by me for the purpose of providing, coordinating, or managing your health care treatment and any related services. This may include coordination or management of your health care with a third party, consultation or supervision activities with other health care providers, or referral to another provider for health care services.

Payment. I may use your PHI to obtain payment for your health care services. This may include providing information to a third party payor, or, in the case of unpaid fees, submitting your name and amount owed to a collection agency.

Healthcare Operations. I may use or disclose your PHI in order to support the business activities of my professional practice including; disclosures to others for health care education, or to provide planning, quality assurance, peer review, or administrative, legal, financial, or actuarial services to assist in the delivery of health care, provided I have a written contract with the business that prohibits it from re-disclosing your PHI and requires it to safeguard the privacy of your PHI. I may also contact you to remind you of your appointments.

Other Uses and Disclosures That Do Not Require Your Authorization

Required by Law. I may use or disclose your PHI to the extent that the use or disclosure is required by law, made in compliance with the law, and limited to the relevant requirements of the law. Examples of this type of disclosure include healthcare licensure related reports, public health reports, and law enforcement reports. Under the law, I must make certain disclosures of your PHI to you upon your request. In addition, I must make disclosures to the US Secretary of the Department of Health and Human Services for the purpose of investigating or determining my compliance with the requirements of privacy rules.

Health Oversight. I may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies and organizations that provide financial assistance to the program (such as third-party payors) and peer review organizations performing utilization and quality control. If I disclose PHI to a health oversight agency, I will have an agreement in place that requires the agency to safeguard the privacy of your information.

Abuse or Neglect. I may disclose your PHI to a state or local agency that is authorized by law to receive reports of abuse or neglect. However, the information we disclose is limited to only that information which is necessary to make the required mandated report.

Deceased Clients. I may disclose PHI regarding deceased clients for the purpose of determining the cause of death, in connection with laws requiring the collection of death or other vital statistics, or permitting inquiry into the cause of death.

Research. I may disclose PHI to researchers if (a) an Institutional Review Board reviews and approves the research and a waiver to the authorization requirement; (b) the researchers establish protocols to ensure the privacy of your PHI; and (c) the researchers agree to maintain the security of your PHI in accordance with applicable laws and regulations.

Criminal Activity or Threats to Personal Safety. I may disclose your PHI to law enforcement officials if I reasonably believe that the disclosure will avoid or minimize an imminent threat to the health or safety of yourself or any third party.

Compulsory Process. I may be required to disclose your PHI if a court of competent jurisdiction issues an appropriate order, and if the rule of privilege has been determined not to apply. I may be required to disclose your PHI if I have been notified in writing at least fourteen days in advance of a subpoena or other legal demand, no protective order has been obtained, and a competent judicial officer has determined that the rule of privilege does not apply.

Essential Government Functions. I may be required to disclose your PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and

national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

Law Enforcement Purposes. I may be authorized to disclose your PHI to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if I suspect that criminal activity caused the death; (5) when I believes that protected health information is evidence of a crime that occurred on my premises; and (6) in a medical emergency not occurring on my premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Psychotherapy Notes. If kept as separate records, I must obtain your authorization to use or disclose psychotherapy notes with the following exceptions. I may use the notes for your treatment. I may also use or disclose, without your authorization, the psychotherapy notes for my own training, to defend myself in legal or administrative proceedings initiated by you, as required by the Washington Department of Health or the US Department of Health and Human Services to investigate or determine my compliance with applicable regulations, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight, for the lawful activities of a coroner or medical examiner or as otherwise required by law.

Uses and Disclosures of PHI With Your Written Authorization

Other uses and disclosures of your PHI will be made only with your written authorization. I will not make any other uses or disclosures of your psychotherapy notes, I will not use or disclosure your PHI for marketing proposes, and I will not sell your PHI without your authorization. You may revoke your authorization in writing at any time. Such revocation of authorization will not be effective for actions I may have taken in reliance on your authorization of the use or disclosure.

Your Rights Regarding Your PHI

You have the following rights regarding PHI that I maintain about you. Any requests with respect to these rights must be in writing. A brief description of how you may exercise these rights is included.

Right of Access to Inspect and Copy. You may inspect and obtain a copy of your PHI that is contained in a designated record set for as long as I maintain the record. A "designated record set" contains medical and billing records and any other records that I use for making decisions about you. Your request must be in writing. I may charge you a reasonable cost-based fee for the copying and transmitting of your PHI. I can deny you access to your PHI in certain circumstances. In some of those cases, you will have a right of recourse to the denial of access. Please contact me if you have questions about access to your medical record.

Right to Amend. You may request, in writing, that I amend your PHI that has been included in a designated record set. In certain cases, I may deny your request for an amendment. If I deny your request for amendment, you have the right to file a statement of disagreement with me. I may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal.

Right to an Accounting of Disclosures. You may request an accounting of disclosures made for treatment purposes or made as a result of your authorization, for a period of up to six years, excluding disclosures made to you. I may charge you a reasonable fee if you request more than one accounting in any 12-month period. Please contact me if you have questions about accounting of disclosures.

Right to Request Restrictions. You have the right to ask me not to use or disclose any part of your PHI for treatment, payment or health care operations or to family members involved in your care. Your request for

restrictions must be in writing and I am not required to agree to such restrictions. Please contact me if you would like to request restrictions on the disclosure of your PHI.
You also have the right to restrict certain disclosures of your PHI to your health plan if you pay out of pocket in full for the health care I provide to you.
Right to Request Confidential Communication. You have the right to request to receive confidential communications from me by alternative means or at an alternative location. I will accommodate reasonable written requests. I may also condition this accommodation by asking you for information regarding how payment will be handled or specification of an alternative address or other method of contact. Please contact me if you would like to make this request.
Right to a Copy of this Notice. You have the right to obtain a copy of this notice from me. Any questions you have about the contents of this document should be directed to me.
Right to Opt Out. You have the right to choose not to receive fundraising communications. However, I will not contact you for fundraising purposes.
Right to Notice of Breach. You have the right to be notified of any breach of your unsecured PHI.

Electronic Records Disclosure

I keep and store records for each client in a record-keeping system produced and maintained by Simple Practice LLC. This system is "cloud-based," meaning the records are stored on servers which are connected to the Internet. Here are the ways in which the security of these records is maintained:

- I have entered into a HIPAA Business Associate Agreement with Simple Practice LLC. Because of this agreement, Simple Practice LLC is obligated by federal law to protect these records from unauthorized use or disclosure.
- The computers on which these records are stored are kept in secure data centers, where various physical security measures are used to maintain the protection of the computers from physical access by unauthorized persons.
- Simple Practice LLC employs various technical security measures to maintain the protection of these records from unauthorized use or disclosure.
    - SimplePractice always transmits account information securely with multiple layers of encryption.
    - Their servers are housed in a secure facility protected by proximity readers, biometric scanners, and security guards 24 hours a day, 7 days a week, 365 days a year.
    - SimplePractice runs thousands of tests on its own software to ensure security. They scan their ports, test for SQL injection, and protect against cross-site scripting.
- I have my own security measures for protecting the devices that I use to access these records:
    - On computers, I employ firewalls, antivirus software, passwords, and disk encryption to protect the computer from unauthorized access and thus to protect the records from unauthorized access.
    - With mobile devices, I use passwords, remote tracking, and remote wipe to maintain the security of the device and prevent unauthorized persons from using it to access my records.

Here are things to keep in mind about my record-keeping system:

- While my record-keeping company and I both use security measures to protect these records, their security cannot be guaranteed.
- Some workforce members at Simple Practice LLC, such as engineers or administrators, may have the ability to access these records for the purpose of maintaining the system itself. As a HIPAA Business Associate, Simple Practice LLC is obligated by law to train their staff on the proper maintenance of confidential records and to prevent misuse or unauthorized disclosure of these records. This protection cannot be guaranteed, however.

- My record-keeping company keeps a log of my transactions with the system for various purposes, including maintaining the integrity of the records and allowing for security audits. These transactions are kept for as long as Catalyst Counseling has an account with Simple Practice LLC.

To help prevent the loss or damage of records, I keep backups of them using an online backup service produced and maintained by G Suite Business. This service is "cloud-based," meaning the backups are stored on computers which are connected to the Internet. Here are the ways in which the security of these backups is maintained:

- I have entered into a HIPAA Business Associate Agreement with G Suite Business. Because of this agreement, G Suite Business is obligated by federal law to protect these backups from unauthorized use or disclosure.
- The computers on which these backups are stored are kept in secure data centers, where various security measures are used to maintain the protection of the computers from physical access by unauthorized persons.
- G Suite Business employs various security measures to maintain the protection of these backups from unauthorized use or disclosure.
    - In addition to supporting HIPAA compliance, the G Suite Core Services are audited using industry standards such as ISO 27001, ISO 27017, ISO 27018, and SOC 2 and SOC 3 Type II audits, which are the most widely recognized, internationally accepted independent security compliance audits.

Here are things to keep in mind about my record-keeping system:

- While my data backup company and I both use security measures to protect these records, their security cannot be guaranteed.
- Some workforce members at G Suite Business, such as engineers or administrators, may have the ability to access these records for the purpose of maintaining the system itself. As a HIPAA Business Associate, G Suite Business is obligated by law to train their staff on the proper maintenance of confidential data and to prevent misuse or unauthorized disclosure of these records. This protection cannot be guaranteed, however.

Disclosure Regarding Third-Party Access to Communications

Please know that if we use electronic communications methods, such as email, texting, online video, and possibly others, there are various technicians and administrators who maintain these services and may have access to the content of those communications. In some cases, these accesses are more likely than in others.

Of special consideration are work email addresses. If you use your work email to communicate with me, your employer may access our email communications. There may be similar issues involved in school email or other email accounts associated with organizations that you are affiliated with. Additionally, people with access to your computer, mobile phone, and/or other devices may also have access to your email and/or text messages. Please take a moment to contemplate the risks involved if any of these persons were to access the messages we exchange with each other.

Communications Policy

When you need to contact Catalyst Counseling for any reason, these are the most effective ways to get in touch in a reasonable amount of time:

- By phone (425-998-9769.) You may leave messages on the voicemail, which is confidential.
- By secure text message (see below for details.)
- By secure email (see below for details.)
- If you wish to communicate with me by normal email or normal text message, please read and complete the Consent For Non-Secure Communications form included with these office policies.

I subscribe to the following services that can allow us to communicate more privately through the use of encryption and other privacy technologies. None of them will cost you money, but each requires some setup before they can be used. Please ask if you would like to use any of these services:

- Encrypted email.
- Secure text messaging. This service can be used on a computer or smartphone.
- A secure "client portal," where you can fill out demographic information and other forms.
- Secure online video chat software.

If you need to send a file such as a PDF or other digital document, please send using the secure email service or print and fax it to 844-837-1339. Please refrain from making contact with me using social media messaging systems such as Facebook Messenger or Twitter. These methods have very poor security and I am not prepared to watch them closely for important messages from clients. It is important that we be able to communicate and also keep the confidential space that is vital to therapy. Please speak with me about any concerns you have regarding my preferred communication methods.

Contact Information

Catalyst Counseling acts as our own Privacy and Security Officer. If you have any questions about this Notice of Privacy Practices, please contact our Privacy and Security Officer:

Katherine E. Walter, MSW LICSW
Catalyst Counseling
17330 135TH Ave NE, Suite 2B
Woodinville, WA 98072
(425) 998-9769

Complaints

If you believe I have violated your privacy rights, you may file a complaint in writing with me, as my own Privacy Officer, as specified above. You also have the right to file a complaint in writing to the Washington Department of Health or to the US Secretary of Health and Human Services. I will not retaliate against you in any way for filing a complaint.

Effective Date

Effective date of this notice: December 14, 2016