

Data Privacy

Diverse Mental Health Response LLC (hereinafter referred to as “Company” or “TP Safe House”) adopts the following policy:

TP Safe House follows the “Data Privacy - Notice of Privacy Practices - HIPAA - MHRA” policy attached and incorporated by reference. Specifically, this policy and notice complies with all applicable state and federal law. The Company’s use of electronic record keeping or electronic signatures does not alter a license holder’s obligations to comply with applicable state and federal law.

A recipient or client must use the “FORM - Minnesota Standard Consent form to release health information” for all releases of the client’s health record, to document valid permission from the client. This form is available electronically and immediately upon request.

Staff and clients have access to use the “FORM - Revocation of Authorization to Disclose Health Information” to promptly document a client’s revocation of consent to disclose the client’s health record. This form is available electronically and immediately upon request.

Legal Authority - ([Minnesota Statutes, section 245I.03, subd. 10](#))

Notice of Privacy Practices

This notice describes how health information about you, the patient, may be used and disclosed by us, the Company (“We”, “us”, “Company”), and how you can get access to this information. Please review it carefully.

We are required by law to maintain the privacy of your protected health information (PHI) and to provide you with notice of your privacy rights and my legal duties and privacy practices with respect to your PHI. We are required to abide by the terms of this notice with respect to your PHI but reserve the right to change the terms of this notice and make the new notice provisions effective for all PHI that we maintain. We will provide you with a copy of the revised notice.

Understanding Your Personal Health Information

Each time you visit a hospital, physician, mental health professional, or other health care provider, a record of your visit is made. Typically, this record contains your symptoms; examination and test results; diagnoses; and treatment plan. This information, often referred to as your health or medical record, serves as a:

- Basis for planning your care and treatment.

Data Privacy

- Means of communication among the many health professionals who contribute to your care.
- Legal document describing the care you received.
- Means by which you or a third-party payer can verify that services billed were actually provided a tool in educating health professionals.
- Source of data for medical research.
- Source of information for public health officials charged with improving the health of the nation, a source of data for facility planning and marketing.
- Tool with which we can assess and continually work to improve the care we render and the outcomes we achieve.

Understanding what is in your record and how your health information is used helps you to:

- Means to ensure its accuracy.
- Way to better understand who, what, when, where, and why others may access your health information.
- Means to make more informed decisions when authorizing disclosure to others.

Your Health Information Rights

Although your health record is the physical property of my practice, the facility that compiled it, the information belongs to you. You have the following privacy rights:

1. The right to request restrictions on the use and disclosure of your PHI to carry out treatment, payment, or health care operations.
2. In connection with any patient directory, the right to request restrictions on the use and disclosure of your name, location at this treatment facility, description of your condition and your religious affiliation. We do not maintain a patient directory.
3. To receive confidential communication of your PHI unless we determine that such disclosure would be harmful to you.
4. To inspect and copy your PHI unless we determine in the exercise of professional judgment that the access requested is reasonably likely to endanger your life, emotional or physical safety or that of another person. You may request copies of your PHI by providing the Company with a written request for such copies.
5. To amend your PHI upon your written request to the Company setting forth your reasons for the requested amendment. The Company has the right to deny the request if the information is complete or has been created by another entity.

Data Privacy

We are required to act on your request to amend your PHI within sixty (60) days but this deadline may be extended for another thirty (30) days upon written notice to you. If we deny your requested amendment, we will provide you with written notice of the decision and the basis for the decision. You will then have the right to submit a written statement disagreeing with the Company's decision which will be maintained with your PHI. If you do not wish to submit a statement of disagreement,

you may request that we provide your request for amendment and our denial with any future disclosures of your PHI.

6. Upon request to receive an accounting of disclosures of your PHI made within the past 6 years of your request for an accounting. Disclosures that are exempt from the accounting requirement include the following:

- Disclosures necessary to carry out treatment, payment, and health care operations (most common disclosure).
- Disclosures made to you upon request.
- Disclosures made pursuant to your authorization.
- Disclosures made for national security or intelligence purposes.
- Permitted disclosures to correctional institutions or law enforcement officials.
- Disclosures that are part of a limited data set used for research, public health, or health care operations. We are required to act on your request for an accounting within sixty (60) days but this deadline may be extended for another thirty (30) days upon written notice to you of the reason for the delay and the date by which we will provide the accounting. You are entitled to one (1) accounting in any twelve (12) month period free of charge. For any subsequent request in a twelve (12) month period you will be charged a reasonable fee allowed by law for each page copied and you will be expected to pay for the copies at the time you pick them up.

7. To receive a paper copy of this privacy notice even if you agreed to receive a copy electronically.

8. To pay out-of-pocket for a service and the right to require that the Company not submit PHI to your health plan.

9. To be notified of a breach of your unsecured PHI.

10. The right to complain to the Company's privacy officer and to the Secretary of the U.S. Department of Health and Human Services if you believe your privacy rights have been violated. You may submit your complaint to the Company in writing setting out the alleged violation. The Company is prohibited by law from retaliating against you in any way for filing a complaint with me or Health and Human Services.

Data Privacy

11. If your records are maintained electronically, the right to receive a copy of your PHI in an electronic format and to direct in writing that a third party receive a copy of your PHI in an electronic format. As a default, we transmit our records electronically.

12. We must protect your client records against loss, tampering, or unauthorized disclosure of confidential client data according to the Minnesota Government Data Practices Act, chapter 13; the privacy provisions of the Minnesota health care programs provider agreement; the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191; and the Minnesota Health Records Act, sections [144.291](#) to [144.298](#).

Uses and Disclosures

It is the Company's policy to protect the confidentiality of your PHI to the best of our ability and to the extent permitted by law. There are times however, when use or disclosure of your PHI is permitted or mandated by law even without your authorization.

Situations where we are not required to obtain your consent or authorization for use or disclosure of your PHI include the following circumstances:

- By Company or office staff for treatment, payment, or health care operations as they relate to you.
- In the event of an emergency to any treatment provider who provides emergency treatment to you.
- To defend Company or its agents in a legal action or other proceeding brought by you against the Company or its agents.
- When required by the Secretary of the Department of Health and Human Services in an investigation to determine the Company's compliance with the privacy rules.
- When required by law insofar as the use or disclosure complies with and is limited to the relevant requirements of such law.
 - Examples: To a public health authority or other government authority authorized by law to receive reports of child abuse or neglect.
- If the Company or providers reasonably believe an adult individual to be the victim of abuse, neglect or domestic violence, to a governmental authority, including a social services agency authorized by law to receive such reports to the extent the disclosure is required by or authorized by law or you agree to the disclosure and we believe that in the exercise of professional judgment disclosure is necessary to prevent serious harm to you or other potential victims.

In the course of any judicial or administrative proceeding in response to:

- An order of a court or administrative tribunal so long as only the PHI expressly authorized by such order is disclosed.

Data Privacy

- A subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal so long as reasonable efforts are made to give you notice that your PHI has been requested or reasonable efforts are made to secure a qualified protective order, by the person requesting the PHI.
- Child custody cases and other legal proceedings in which your mental health or condition is an issue are the kinds of suits in which your PHI may be requested. In addition we may use your PHI in connection with a suit to collect fees for services.
- In compliance with a court order or court ordered warrant, or a subpoena or summons issued by a judicial officer, a grand jury subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by law provided that the information sought is relevant and material to a legitimate law enforcement inquiry and the request is

specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought and de-identified information could not reasonably be used.

- To a health oversight agency for oversight activities authorized by law as they may relate to the Company or its agents (i.e., audits; civil, criminal, or administrative investigations, inspections, recertifications, legal compliance, licensure, or disciplinary actions; civil, administrative, or criminal proceedings or actions).
- To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or performing other duties as authorized by law.
- To funeral directors consistent with applicable law as necessary to carry out their duties with respect to the decedent.
- To the extent authorized by and the extent necessary to comply with laws relating to workers compensation or other similar programs established by law.
- If use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
- To a public health authority that is authorized by law to collect or receive such information for the purposes of preventing or controlling a disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth, death, and the conduct of public surveillance, public health investigations, and public health interventions.
- To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such persons as necessary in the conduct of a public health intervention or investigation.
- To a public health authority or other appropriate governmental authority authorized by law to receive reports of child abuse or neglect.

Data Privacy

- To a law enforcement official if we believe in good faith that the PHI constitutes evidence of criminal conduct that occurs on the Company premises.
- To authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act and implementing authority.
- To Business Associates under a written agreement requiring Business Associates to protect the information. Business Associates are entities that assist with or conduct activities on our behalf including individuals or organizations that provide legal, accounting, billing, administrative, and similar functions.

We may contact you with appointment reminders or information about treatment alternatives or other health related benefits and services that may be of interest to you.

Privacy

The Company shall maintain your privacy to the maximum extent that it can, but there may be lapses in confidentiality and privacy when IRTS services are provided. IRTS is a community-based service. IRTS includes services provided outside of a formal, closed-office setting at a provider's office. I understand that in a new setting, not all the variables in providing services are known. If at any point I feel overwhelmed or uncomfortable or that my privacy is not to the level I would like, I will respect my limitations and I will notify the Company or its providers as appropriate. In addition, privacy and confidentiality may be compromised when we are in a public setting or the community, and I waive confidentiality and privacy for any reasonable lapses, such as a family member or friend being present in the setting or members of the public out in the community. If I have issues with privacy, I will immediately report those to the Company's privacy officer and this will be noted in my file, and we will initiate a meeting to determine the best next steps.

Family Engagement - Minnesota Health Records Act

Paragraph 1

1. Upon the written request of a spouse, parent, child, or sibling of a patient being evaluated for or diagnosed with mental illness, our Company shall inquire with you whether you wish to authorize a specific individual to receive information regarding your current and proposed course of treatment. If you so authorize, the Company shall communicate to the designated individual the patient's current and proposed course of treatment. A valid release of information shall be filled out to document this authorization.

Paragraph 2

Data Privacy

2. (A) Notwithstanding paragraph #1, or a proper release or disclosure of records under Minn section [144.293](#), a provider providing mental health care and treatment may disclose health record information about a patient to a family member of the patient or other person who requests the information if all of the following six statements are true:

- (1) the request for information is in writing;
- (2) the family member or other person lives with, provides care for, or is directly involved in monitoring the treatment of the patient;
- (3) the involvement under clause (2) is verified by the patient's mental health care provider, the patient's attending physician, or a person other than the person requesting the information, and is documented in the patient's medical record;
- (4) before the disclosure, the patient is informed in writing of the request, the name of the person requesting the information, the reason for the request, and the specific information being requested;
- (5) the patient agrees to the disclosure, does not object to the disclosure, or is unable to consent or object, and the patient's decision or inability to make a decision is documented in the patient's medical record; AND
- (6) the disclosure is necessary to assist in the provision of care or monitoring of the patient's treatment.

(B) The information disclosed under this section is limited to diagnosis, admission to or discharge from treatment, the name and dosage of the medications prescribed, side effects of the medication, consequences of failure of the patient to take the prescribed medication, and a summary of the discharge plan.

(C) If a provider reasonably determines that providing information under this section would be detrimental to the physical or mental health of the patient or is likely to cause the patient to inflict self harm or to harm another, the Company shall not disclose the information.

(D) This paragraph #2, does not apply for disclosures made under paragraph #1, or disclosures for a medical emergency, including a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency;

Email, Phone and Text Communications

Company may offer the use of email, text and phone communications to provide services to you. You will need to sign your initials on page 93 to opt into this service. You may sign your initials electronically or handwritten signature with a staff member. By providing your phone number and opting into SMS/text communication, you agree to receive automated text messages from Diverse Mental Health Response LLC. Message frequency varies. Message and data rates may apply. You may opt out of SMS/text messaging at any time by responding STOP to any SMS/text messages or contacting a company staff of your desire. View our Privacy Policy [link].

Data Privacy

Based on the inherent risk of communication via email, texting and phone, as well as the unpredictability and inability to control third-parties who may attempt to gain access to emails and texts, or passwords in an unauthorized manner, Company has not, cannot, and will not guarantee the security and confidentiality of text, phone or email communications. As such, Company will not be liable for improper disclosure of any information that is contained in email, text or phone communication, which disclosure is not caused by Company's intentional misconduct, assuming you have opted in to receive these types of communications with your initials below. Additionally, company collects phone numbers only for the purpose of sending SMS messages. SMS opt-in data and consent will not be shared with or sold to third parties. The only circumstances in which mobile information including phone numbers may be shared to a third party are if we partner with a third-party service provider to manage our site/company and to comply with any legal obligations by legal authorities.

Counterparts; Electronic Signature and Delivery.

This Policy, and any Company Documents for providing services, may be executed in any number of counterparts, each of which when so executed and delivered shall be deemed an original, but together shall constitute one and the same instrument. You acknowledge and agree that (i) a facsimile, electronically transmitted via PDF/email transmission, or similar copy of a handwritten signature or an electronic signature (as defined in the Uniform Electronic Transactions Act (Minn. Stat. Ch. 325L)) shall have the effect of an original signature; and (ii) signature pages to this Agreement, or any Company documents, may be delivered by electronic transmission and shall be as binding as original counterparts. You understand that an electronic signature has the same legal effect and can be enforced in the same way as a written signature. (MN Statute 302A.015).

The Company may make use of electronic signatures to provide services.

If you have any questions and would like additional information you should bring this to our attention at the first opportunity.

The designated Privacy Officer for our Company and will be glad to respond to your questions or request for information.

Company Privacy Officer Name: Xeng Ying Pha

Email: diversehr@gmail.com

Address: 1400 Queen Ave N

Minneapolis, MN 55411

Phone: 651-425-1614

Data Privacy

Client Consent Form

I understand that as part of my health care, the Company originates and maintains health records describing my health history, symptoms, evaluations and test results, diagnosis, treatment, and any plans for future care or treatment. I understand that this information is utilized to plan my care and treatment, to bill for services provided to me, to communicate with other health care providers, and to carry out other routine health care operations such as assessing quality and reviewing competence of health care professionals.

I have been provided and have received Company's Notice of Privacy Practices and have had time to ask questions and seek clarifications.

[Optional] I consent to receive services via phone text messaging. Initials _____

[Optional] I consent to receive services via email. Initials _____

[Optional] I consent to receive services via phone call. Initials _____

Signature of Client or Legal Representative: _____

Date: _____

Policy reviewed and authorized by: Xeng Ying Pha, Owner

Policy Initiated on Date:

Policy revisions:

Date policy revision initiated*	Staff Name	Comments
---------------------------------	------------	----------

Data Privacy

*The license holder must complete and document a review of policies and procedures every two years and update policies and procedures as necessary