LIST OF RISKS FOR TELEHEALTH & EMAIL COMMUNICATION

TELEHEALTH

ReDiscover may provide telehealth services as agreed upon by clients. ReDiscover will use reasonable means to protect the security and confidentiality of teleheath services. However, there are certain risks that may be beyond ReDiscover's control. If client agrees to using telehealth services, client understands and accepts the risks listed below.

Risks include, but are not limited to:

- Potential information inaccuracies due to incomplete audio or data feed.
- Unauthorized access to information during collection, transmission, or storage due to hacking or using unsecure systems.

EMAIL COMMUNICATION

ReDiscover offers clients the opportunity to communicate by email. ReDiscover will use reasonable means to protect the security and confidentiality of email information sent and received. ReDiscover uses encryption software as a security mechanism for email communications with Protected Health Information (PHI). However, because of the risks outlined below, ReDiscover cannot guarantee the complete security and confidentiality of email communication.

For the purpose of this document, 'Client' will be used to refer to any ReDiscover client or personal representative of client whose email information is provided. Client should be aware that transmitting email communication poses risks that may be beyond ReDiscover's control. If client chooses to provide ReDiscover with their email address at any time for any purpose(s), client understands and accepts the risks listed below.

Risks include, but are not limited to:

- The client is responsible for informing ReDiscover of any changes in email address.
- The privacy and security of all email communication cannot be guaranteed.
- Email communication is not an appropriate substitute for clinical examinations. The client is responsible for following up on ReDiscover's email and for scheduling appointments where warranted.
- ReDiscover may have a legal right to inspect and keep emails that pass through their system.
- Email is easier to falsify than handwritten or signed hard copies. In addition, it is impossible to verify the true identity of the sender, or to ensure that only the recipient can read the email once it has been sent.
- Emails can introduce viruses into a computer system, and potentially damage or disrupt the computer.
- Email can be forwarded, intercepted, circulated, stored or even changed without the knowledge or permission of ReDiscover or the client. Email senders can easily misaddress an email, resulting in it being sent to many unintended and unknown recipients.

- Email is indelible. Even after the sender and recipient have deleted their copies of the email, back-up copies may exist on a computer or in cyberspace.
- Use of email to discuss sensitive information can increase the risk of such information being disclosed to third parties.
- Email can be used as evidence in court.
- If client chooses to receive PHI communication unencrypted either due to issues of receipt or other preferences, client understands & accepts that there may be higher risks involved.
- Although ReDiscover will attempt to read and respond promptly to an email from the client, ReDiscover cannot guarantee that any particular email will be read and responded to within any particular period of time. Thus, the client should refrain from using email for medical emergencies or other time-sensitive matters.
- If the client's email requires or invites a response from ReDiscover and the client has not received a response within a reasonable time period, it is the client's responsibility to follow up to determine whether the intended recipient received the email and when the recipient will respond.
- ReDiscover is not responsible for information loss due to technical failures associated with the client's email software or internet service provider.