HIPAA (Health Insurance Portability and Accountability Act) regulations and my professional code of ethics require that I keep your PHI (Protected Health Information) private and secure. Email and texting is a very convenient way to handle administrative issues like scheduling or receipt requests, however, they are not 100% secure. Some of the potential risks you might encounter include:

- Misdelivery of email to an incorrectly typed email address.
- Email accounts can be 'hacked', giving a third party access to content and addresses.
- Email provider/servers (ie, gmail, comcast, yahoo) may keep a record of each email where it might be accessible to employees.
- Your cell phone may be lost or stolen and texts/emails read.

For these reasons, we will not use email or text to discuss clinical issues (ie, the important things discussed in sessions).

If *you* are comfortable doing so, we are happy to use email/text to handle administrative matters like scheduling and billing.

If you are *not* comfortable with these risks, we can communicate through the HIPAA compliant email portal in Simple Practice or telephone.

No mobile information will be shared with third parties/affiliates for marketing/promotional purposes. All the above categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties.

By checking the box below, I understand the potential risks if I should communicate via email or text.