Little Lamp Christian Counseling LLC

DATA BREACH POLICY

A data breach occurs when an unauthorized person gains access to information that is meant to be confidential, private, protected or sensitive. Though rare in occurrence, and despite heightened internet security, breaches can and do happen. The following are ways clients of Little Lamp Christian Counseling LLC could be potential victims of a breach. In every case, the counselor will inform the affected clients immediately and take all necessary steps to ensure the safety of the client to the full letter of the law.

Doxy.me
This company uses Doxy.me for videoconferencing and form collection. Doxy.me is a telemedicine/videoconferencing platform that implements state of the art security and encryption protocols to assure that data integrity and privacy is maintained. As a result, doxy.me complies with HIPAA, GDPR, PHIPA/PIPEDA, & HITECH requirements. Doxy.me does not store patient information. In the event the breach was the fault of Doxy.me, the counselor will receive an email notice from Doxy.me as soon as Doxy.me are made aware.

Stripe Inc.
This company uses Stripe Inc. to conduct payments for service. Stripe, Inc. is an American multinational financial services and software as a service company. Stripe is certified as a PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. This includes both Stripe's Card Data Vault (CDV) and the secure software development of their integration code. Stripe Terminal is certified to the EMVCo Level 1 and 2 standards of EMV. In the event the breach was the fault of Stripe Inc., the counselor will receive an email notice from Stripe Inc., as soon as Stripe Inc. are made aware.

Venmo (Business Profile – PayPal, Inc.)
This company uses Venmo for Business, a service operated by PayPal, Inc., to process payments for services. PayPal, Inc. is a globally recognized financial technology company that provides digital payment processing and related financial services. Venmo transactions are processed through PayPal's secure payment infrastructure, which is designed to comply with applicable PCI-DSS (Payment Card Industry Data Security Standard) requirements for handling sensitive payment data. In the event of a data security incident or breach attributable to Venmo or PayPal, the company will notify the counselor in accordance with their established incident response and notification procedures once they become aware of the issue.

Counselor or Client Error
Another possibility is a breach due to counselor or client error. To lessen this possibility, Little Lamp Christian Counseling LLC has researched companies for those that adhere to HIPAA standards and has signed BAA's with each. Little Lamp Christian Counseling LLC uses a dedicated laptop, disconnected from any cloud services and protected with Norton security for client sessions and notes. All notes are protected with password encryption. Little Lamp Christian Counseling LLC will never ask for client Social Security Numbers.

Little Lamp Christian Counseling LLC

The following is what to do in case a Data Breach does occur. (This information was taken from Experian Information Solutions Inc.):

1. Stay Alert
Hang on to any unusual mail or emails, such as IRS tax notices, bills or statements from unfamiliar lenders.

- Try to file your taxes early, before scammers can. Tax identity theft happens when someone uses your social security number to get a tax refund or a job.

2. Secure Accounts

- A thief who's obtained login information for one account could be able to use the same information to break into others if the individual uses the same login information for all websites, so individuals may want to update other website logins as well. Using a free password manager will make this process easier. Consider activating two-factor authentication on accounts which make it much harder for password thieves to gain access.

3. Initiate a Fraud Alert

- A fraud alert notifies any lender processing a credit application in the individuals' name that the individual may be a victim of fraud or identity theft and requests that they verify the applicant is really the client before moving ahead with the application. A fraud alert will stay on the individuals' credit report for one year.

4. Monitor Financial Accounts and Credit Reports
Staying aware of unusual or unexpected activity on an account lets the individual detect potential scams early and allows the individual to report or investigate them promptly. Checking the individuals' credit report also can help to identify any unusual activity related to credit fraud and identity theft, such as the creation of loan or credit card accounts the individual doesn't recognize and the addition of unfamiliar addresses to personal information.

- If you have an account with the company that experienced the breach, log in to the account and change your password. If possible, also change your username.
- If you can't log in, contact the company. Ask them how you can recover or shut down the account.
- If you use the same password anywhere else, change that too.
- If it is a financial site, or your credit card information is stored on the site, check your bank account for any charges you don't recognize.
- If your bank account information was exposed, contact your bank to close the account and open a new one.
- If credit or debit card information was exposed, contact your bank or credit card company to cancel your card and request a new one.

5. Freeze or Lock Credit File
Though potentially more inconvenient than a fraud alert, the individual might consider applying a free security freeze or lock, which limits access to a credit report at a specific credit bureau. The individual can freeze credit reports at Experian, Equifax and TransUnion. Freezing or locking credit at all three bureaus helps protect the credit file from scammers and other criminals who may apply for credit in the individuals' name. However, it will also prevent creditors from accessing the credit for legitimate credit applications. If the individual wants to allow a lender to view a frozen credit report (as when applying for a credit card or loan), the individual must first unfreeze the credit reports. Once the process is complete, it is recommended, that the individual freeze or lock credit accounts again. If the company responsible for exposing your information offers you free credit monitoring, take advantage of it.