North Star
COUNSELING SERVICES

North Star Mental Health Counseling Services
368 Veterans Memorial Hwy Ste 3, Commack, NY
P: (631) 533-0315 | **F:** (855) 752-5170
E: hello@northstarlongisland.com
W: northstarlongisland.com

INFORMATION AND RISKS OF NON-SECURE COMMUNICATION METHODS PERTAINING TO CLIENTS' PHI (PROTECTED HEALTH INFORMATION)

The purpose of this document is to explain the key differences between various communication methods, specifically non-secure methods of communication, such as, SMS-text messages and non-encrypted emails versus more secure methods of communication, such as,encrypted emails, secure encrypted HIPAA portals, and phone calls. It is crucial to understand these distinctions, as clients' awareness of the associated risks is essential for you to make informed decisions about your preferred communication methods. By highlighting the potential risks involved in non-secure communication, clients like yourself can make informed choices and determine your comfort level with the accompanying risks. Protecting the confidentiality of clients' protected health information (PHI) remains our utmost priority, and we aim to provide secure communication options that best suit our clients' needs.

Here's an outline highlighting why non-secure methods of communication, such as SMS-text messages and non-encrypted emails, are considered less secure from a HIPAA and encryption perspective compared to encrypted email, secure encrypted HIPAA portals, and phone calls.

It is important to note that even when utilizing SMS-text messages, North Star uses a company/service named Talkroute and North Star has a Business Associates Agreement with Talkroute. This means that text messages are stored within a HIPAA compliant matter, but nevertheless, due to the inherent nature of how SMS text messages are sent/received, while in transit, they are not encrypted and therefore have increased security risks, especially as compared to encrypted emails, encrypted portals, or phone calls.

On the other hand, for emails, North Star uses Google Workspace as our email provider, and has a Business Associates Agreement with Google Workspace, rendering this a HIPAA compliant solution for storing email and data. As an extra safeguard, North Star also utilizes a company/service named LuxSci (of whom we also have a Business Associates Agreement with), who specialize in securing and encrypting outbound emails while in transit as well as when storing email data. This said, we of course do not have control over the platforms, services, and settings that our clients use to send, receive, and store their emails, and therefore cannot guarantee encryption for emails that we receive from clients, as that encryption level would depend on how it was sent from a client, which is outside of our control. Therefore we feel it is quite important to educate our clients on these risks.

Non-Secure Methods of Communication:

SMS-Text Messages and Non-Encrypted Emails:

- Lack of end-to-end encryption: SMS-text messages and non-encrypted emails may travel through various servers and networks, making them susceptible to interception or unauthorized access.
- Risk of accidental disclosure: Messages sent via SMS-text or non-encrypted emails can be inadvertently sent to the wrong recipient, potentially exposing PHI.

North Star Mental Health Counseling Services
368 Veterans Memorial Hwy Ste 3, Commack, NY
P: (631) 533-0315 | **F:** (855) 752-5170
E: hello@northstarlongisland.com
W: northstarlongisland.com

- Storage vulnerabilities: Text messages and emails may be stored on devices or servers, increasing the risk of unauthorized access or data breaches.
- Limited control over message lifespan: Once sent, text messages and emails may remain on devices or servers indefinitely, increasing the potential for unauthorized access in the future.

Secure Methods of Communication:

III. Encrypted Email:
- Strong encryption: Encrypted email services utilize encryption protocols, ensuring that only authorized recipients can decrypt and access the message content.
- Secure access methods: Encrypted email often requires login credentials or secure authentication methods, adding an extra layer of protection.
- Data protection during transmission: Encrypted email ensures that PHI is protected during transit, reducing the risk of interception and unauthorized access.

IV. Secure Encrypted HIPAA-Compliant Portals:
- Enhanced data protection: HIPAA-compliant portals utilize encryption technologies, safeguarding PHI during storage and transmission.
- Access control: HIPAA portals typically require user authentication and secure login credentials, limiting access only to authorized individuals.
- Secure messaging features: Secure HIPAA portals provide dedicated messaging capabilities, allowing secure communication while ensuring message integrity and confidentiality.

V. Phone Calls
- Real-time communication: Phone calls provide immediate, direct communication, reducing the potential for storage vulnerabilities compared to digital messaging.
- Limited risk of interception: Phone calls generally have a lower risk of interception or unauthorized access, as messages are transmitted in real-time directly between individuals.

We hope that this summary of the advantages and disadvantages of various communication methods in terms of HIPAA compliance and encryption has been informative and helpful. If you have any questions pertaining to any of the above information, please feel free to contact us at (631) 533-0315 or emailing supervisor@northstarlongisland.com. Thank you!