

Policy on the Use of E-Mail and Text Messaging to Communicate Patients' Protected Health Information

Achieve Beyond must maintain the confidentiality its patients' Protected Health Information or "PHI". PHI is information, transmitted or maintained in any form or medium, that relates to the:

- Past, present or future physical or mental health or condition of an individual provision of health care to an individual
- Past, present or future payment for the provision of health care to an individual;
- Identifies the individual in any way, including by name, social security number, finger print, or full face photographic images; and
- Has been created or received by a Covered Entity such as Achieve Beyond

Given that both e-mail and text messaging are dominant forms of communication, extra precaution must be taken when communicating PHI.

General E-mail Precautions

Achieve Beyond employees and contractors may only transmit PHI between Achieve Beyond e-mail addresses, as the company controls all security on the "achievebeyondusa.com" domain.

PHI is never to be transmitted to and from an outside e-mail address. Individuals should never communicate any information regarding a patient's treatment or payment/billing information to or from an outside e-mail address. Nor should an individual communicate a patient's name, social security number, date of birth or images and/or videos of the patient to or from an outside e-mail address.

Exceptions to E-mailing PHI to and from Outside E-mail Addresses

Employees and contractors may e-mail PHI to a parent/guardian of a patient if the parent/guardian gives written consent to e-mail PHI. All employees and contractors should verify that the respective parent/guardian has given written consent to e-mail with the appropriate Program Manager. Direct Service Providers should never directly accept written consent to e-mail from a parent/guardian without first consulting with the appropriate Program Manager.

Individuals may e-mail a password protected attachment (PDF, MS Word, MS Excel, etc) containing PHI to or from an outside e-mail address. PHI should only be contained in the password protected attachment and not in the body of the actual e-mail. The password to the attachment should be provided to the recipient via phone or a follow up e-mail. The password should never be contained in the body of the e-mail carrying the actual attachment.

Text Messaging

PHI should never be transmitted via text message. Information regarding treatment, the patient's name, Social Security number, date of birth or images and/or videos should never be communicated via text message. A Direct Service Provider may confirm treatment times or locations, without using patient name, via text.

Employees and contractors may communicate PHI via text to a parent/guardian of a patient if the parent/guardian gives written consent to text PHI. All employees and contractors should verify that the respective parent/guardian has given written consent to communicate PHI via text with the appropriate Program Manager. Direct Service Providers should never directly accept written consent to text from a parent/guardian without first consulting with the appropriate Program Manager.