

UNENCRYPTED E-MAIL COMMUNICATION and RISK AGREEMENT

Print Person served Legal Name

Person served ID#

Client Preferred Name

Intended emails with PHI are encrypted but when this is not possible, unencrypted emails are allowable per persons served request.

When e-mail is used with a person served, workforce member must advise the person served, his/her parent, legal guardian or authorized representative of the following:

(Person served/Legal Guardian or Authorized Representative is to initial each statement below)

1. There are possible risks of using e-mail, such as technology failure (time lags, hardware defects, and power outages) and confidentiality/security risks (lack of encryption, third party interception, and misdirected e-mail. _____ **Initial**

2. E-mail is treated with a high level of confidentiality, but also is subject to South Community Inc.'s/SCPC's internal monitoring procedures for quality improvement. _____ **Initial**

3. If an e-mail address is shared with others, such as a spouse, significant other, friend etc., the individual will be privileged to the person served's PHI and his/her confidentiality will be compromised. _____ **Initial**

4. The person served should not use e-mail to communicate crises or emergencies. Workforce member advised the person served or his/her parent/legal guardian or authorized representative of emergency procedures including 24-hour phone access. _____ **Initial**

5. You have the right to choose whether your e-mails will be encrypted.

Don't Encrypt Encrypt All E-Mails

Person served/Guardian Signature Date

Staff Signature Date

Print Guardian Name/Authorized Representative (If Applicable)

Print Staff Name

E-mail communications will become part of the persons served electronic health record if applicable. (Scan into e-docs, under correspondence, incoming or outgoing as applicable)