Patient Communications Policy

POLICY STATEMENT:

Aspire ***strongly discourages*** consumers from communicating with their physicians, other healthcare providers, and administrative services via email or SMS text (Short Message Service). Transmitting confidential consumer information by email or text has a number of risks, both general and specific, that consumers should consider before using these methods. Persons we serve are encouraged to use secure messaging within the web portal or other approved Aspire vendors rather than email or text.

Using social media, messaging apps, chat apps, or any method not specifically approved by Aspire to communicate with persons we serve is **strictly prohibited. Only** Aspire approved devices and services with signed Business Associate Agreements (BAA) per HIPAA regulations can be used for communication with persons we serve. For example we do not have agreements with Facebook, Facebook Messenger, Twitter, Snapchat, Instagram, WeChat, LinkedIn, WhatsApp, Skype, Zoom, etc., thus these apps are strictly prohibited and must never be used to communicate with persons we serve.

Before exchanging email or text with a person we serve, an information sheet must be given to them that specifically addresses communication via email and/or text. For those using Telehealth services, the information sheet may be emailed to them. All emails to persons we serve must come or be sent from the Aspire Indiana email system, and all text communications must be sent from an Aspire Indiana owned phone number. It is not necessary to provide the information sheet before Aspire sends non-clinical information like appointment information and requests for documentation needed in order to treat.

As with any external email that contains confidential or Protected Health Information (PHI)/Personally Identifiable Information (PII), it must be encrypted by typing the word “ENCRYPT” in the subject or body of the email. (See policy Email Policy)

Texting of PHI/PII is not permitted and should be limited to appointment reminders with the consent of the person we serve. If a person we serve texts an Aspire staff member clinical information or other PHI, staff must document in the EMR using normal documentation procedures, then delete the text and inform the sender that this should not happen.

PURPOSE:

This policy is enforced to ensure the proper and appropriate use of electronic communications with persons we serve within the organization’s information system. This policy will allow increased opportunity to communicate with a person we serve yet outlines procedures designed to maintain their right to privacy and confidentiality. The policy is also designed to protect the organization from liability in the case of inappropriate exchange of email or SMS text with a person we serve.

PROCEDURE:

Secure Messaging via Portal

- Aspire will request that the Persons we serve provide a current email address to be entered into the Electronic Medical Record (EMR).
- Aspire will request that the Persons we serve register via portal and agree to all stipulations listed on the website prior to any communication.

Email and Texting

- A person we serve must be given the email/texting information form **before** any exchange of confidential information occurs via email/texting. (See Attachment).
- Documentation should be entered in their chart in the Electronic Medical Record (EMR) confirming that the information form has been provided **before** any exchange of confidential information occurs via email or text.
- When discussing the possibility of exchanging email, or in conjunction with presenting the email information form, the staff person must verbally:
    - Explain the risks of using email and texting
    - List the conditions of using email and texting
    - Provide instructions that should be followed to keep email confidential
    - Staff should not delete any emails from persons we serve.

Risk Factors

Inform persons we serve:

- Email and text communications may not remain private and secure
    - Email and text messages can travel much further than planned.
    - Email and text messages could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list.
    - Employers and online services have a right to inspect and keep emails transmitted through their systems
- Email and text messages can be stored, forwarded, intercepted, or even changed without your knowledge or permission or that of the person we serve.
- Email is easier to falsify than handwritten or signed documents.
- Backup copies may exist on a computer, phone, or in the cloud even after you and the other individual delete your copies.
- Emails and text messages are also admissible as evidence in court.
- Email can disrupt or damage the computer of the person we serve if a computer virus is attached to it.
- Email and text messages could be captured electronically enroute if not encrypted.

Conditions of Using Email or SMS Text

Persons we serve should not have an unrealistic expectation about using email or SMS text. Make sure they are aware that certain conditions apply when exchanging email or SMS text.

- Aspire cannot guarantee that electronic communications will be private.

- Aspire will take reasonable steps to protect the confidentiality of consumer email but is not liable for improper disclosure of confidential information not caused by Aspire's gross negligence or want on misconduct.
- Persons we serve are responsible for taking steps to protect themselves from security and privacy violations. For example, it is their responsibility to keep his/her password confidential. Aspire will not be responsible for breaches of confidentiality caused by persons we serve or a third party
- Email contents concerning diagnosis or treatment will be included in the medical record.
- Aspire staff will make every effort to read email and text messages promptly and respond promptly, if warranted. However, there is no guarantee staff will respond to an email within a certain time period. Therefore, do not use email in a medical emergency or any situation that warrants a time sensitive response.
- Following up on any potentially unanswered emails or text is the responsibility of the person we serve.
- Persons we serve are responsible for scheduling any necessary appointments
- Staff will document the information provided via email through normal documentation procedures (i.e. progress notes, etc.).Other staff persons will have access to email information due to job duties. However, the actual message will not be sent to third parties without the consent of the person we serve, except as authorized or required by law.
- Aspire may forward email messages within the organization as necessary for diagnosis, treatment and reimbursement.
- Aspire will not, however, forward the email outside the facility without the consent of the person we serve or as required by law.
- Aspire deems specific healthcare data and information categorized by 42 CFR Part 2 and/or Indiana laws as sensitive thus unauthorized disclosure can be very damaging.
- Persons we serve should be very cautious about using email or text messages for communications concerning diagnosis or treatment of AIDS/HIV infection; other sexually transmissible or communicable diseases, mental health or developmental disability; or alcohol or drug abuse.
- All email messages must be treated with the same degree of confidentiality as other parts of the medical record.

When emailing information outside of Aspire about a person we serve, **never** include their full name in any unencrypted email. (See policy Email Policy for detailed instructions concerning encryption and a full list of information prohibited from inclusion in unencrypted email.)

<u>Instructions for Persons We Serve</u>

- Take steps to keep email confidential, like keeping passwords private and avoid using his/her employer's email system.
- Inform Aspire of any changes to his/her email address or phone number.
- Email communication may only be discontinued via documented patient/client request.
- Receipt of the Email and SMS Texting Communication Information Form is not a mandatory prerequisite for the provision of services.

ENFORCEMENT:

All supervisors, coordinators, and managers are responsible for enforcing this policy.

Employees who violate this policy are subject to discipline up to and including termination from employment, professional discipline, and/or criminal prosecution in accordance with Aspire's disciplinary guidelines.

Approved: Med/Exec. Comm. – 11-8-10
Revised: CCC – 12-21-11
Revised: CCC - 8-19-15
Revised: CCC - 9-16-15
Revised: CCC – 3-16-16
Revised: CCC - 2-21-18
Revised: CCC - 3-2-18, 3-21-18, 5-16-18
Revised: IS/IT - 06-07-22
Approved: Med/Exec. Comm. 7/20/2022
Approved: Aspire Indiana Health, Inc. Board 8/24/2022
Approved: CCC - 2/21/2024
Approved: Aspire Indiana Health, Inc. Board 4/24/2024

Attachment

Email and SMS Texting Communication Information Form

As a person served by Aspire Indiana Health you are being informed of the associated risks, conditions and instructions for communicating with Aspire service providers via email, and are expected to agree to abide by all limitations and agreements outlined. For individuals that wish to communicate with an Aspire service provider via email or sms text, the following information is applicable:

- **Email or sms text will be to persons we serve based on EMR contact information provided during time of registration, the service provider is to be informed of any changes in contact information,**

- **Individuals communicating via email or sms text will use only the email address provided by their Aspire service provider when sending email to Aspire,**

- **Email or sms text exchanged with service providers with content concerning diagnosis or treatment will be included in the medical record and email is not to be used for emergencies or time sensitive matters,**

- **It is the individual's responsibility to protect themselves from security or privacy violations. Aspire is not responsible for breaches of confidentiality caused by a recipient of services or a third party.**

Non-HIPAA Compliant Scenario:☹️
Medical Office Scheduling Team (MOST): Hey there! Just a quick heads-up about your upcoming appointment with Dr. Patel on Feb 10th at 10:00 AM. Can you confirm if you're coming? Thanks!

Patient: Yippers! I will be there. Can you tell me if I have a co-pay? Last time I didn't have to pay a dime.

MOST: Awesome! Thanks for confirming, Sarah! We'll see you on Feb 10th at 10:00 AM. I am looking and see that you owe $45 and have a $20 copay. If you need to reschedule or have any other questions, just give me a shout on my cell phone (765) 574-6380. Have a fantastic day!

Explanation: In this scenario, the medical office sends appointment reminders via text message using informal language and without adhering to HIPAA regulations. The message lacks explicit mention of privacy or confidentiality concerns, and it doesn't provide a secure channel for the patient's response. While it's convenient, it doesn't adhere to HIPAA standards for protecting patient information.

🌟HIPAA Compliant Scenario🙂
Medical Office Scheduling Team (MOST): Hello! This is Aspire Indiana Health about your upcoming appointment scheduled for February 10th. I am reaching out to confirm your appointment or if you need to reschedule I am here to assist. Thank you!

Patient: Thank you so much for reaching out. I am not able to attend. Can we reschedule that appointment for the following week? Same Day of the week and the same time? Can you also let me know if I have an outstanding balance?

MOST: Thank you for rescheduling your appointment! We look forward to seeing you on February 17th at the same time. If you have any questions, please call our office at (877) 574-1254. Unfortunately, I am not able to provide any sensitive information via text. If you need to know your balance please reach out to our billing team at 877-641-8348. Have a great day!

Explanation: In this scenario, the medical office uses a secure text message system to send appointment confirmations to patients who have appointments within 3 days. The message is brief, only containing essential information about the appointment date, along with support for rescheduling. The MOST does not disclose any sensitive medical information, ensuring HIPAA compliance. The patient can respond to the message for confirmation or rescheduling, maintaining patient autonomy and privacy. Understanding that the approval and confirmation have already been captured during a visit with the patient to confirm that the office is using the number on file and has the patient's written approval to communicate via text.