Yakutat Community Health Center

Privacy 5.0-COMMUNICATION OF PROTECTED HEALTH INFORMATION

164.306, 164.312(a)(2)(iv), 164.312(e)(2)(ii), 164.501, 164.502, 164.508, 164.514 (d-f, h)
164.520(b)(1)(iii)(A), 164.522(a-b), 164.528, 164.530(c)(1)

Issue Date: **12-1-2017**
Effective Date: **12-1-2017**
Responsible for Review: **Chief Compliance Officer**
Scheduled Review Date: **12-1-2019**

Purpose

The purpose of the Communications Policy is to provide policies and procedures to safeguard and protect the privacy of Protected Health Information (PHI) while using various mediums of communications. This policy has generalized guidelines and procedures that can be associated with all mediums of communications, and also contains specific procedures due to the different handling of the mediums within a "Communication Matrix". This is an all-inclusive overview of general communication practices that may need to be broken down into separate policies, based on organizational needs.

Policy

PHI can be communicated through various mediums. To comply with the HIPAA Privacy Rule section 164.530 (c)(1) regarding safeguards, and the HIPAA Security Rule section 164.306(a) requiring the safeguarding of the confidentiality, integrity and availability of Electronic PHI (EPHI) an organization creates, receives, maintains or transmits, the Yakutat Community Health Center (YCHC) must have in place appropriate administrative, technical and physical safeguards to protect PHI. It is the policy of YCHC to ensure that PHI is protected from misuse, loss, tampering or use by unauthorized persons. This policy addresses the safeguarding of PHI received, created, used, maintained and/or transmitted via the communication mediums listed using minimum necessary requirements for disclosures of PHI to personnel, patients and their personal representatives, other covered entities, public health officials, business associates, etc. set forth by federal, state and local laws (refer to YCHC's 19.0 Uses and Disclosures Policy). Verification of identity is attained in accordance with the Policy 9.0 Identity Verification Policy prior to release of PHI. Accounting of disclosures of PHI is maintained in compliance with YCHC's Policy. Transmission of EPHI over the YCHC's own network is managed with internal controls such as unique User ID and Password authentication (refer to Security Policy 2.0 User Access Management).

Definitions

Encryption: the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, which identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

•Past, present or future physical or mental health or condition of an individual.
•The provision of health care to an individual.
•The past, present or future payment for the provision of health care to an individual.

Content

Communication will be clear, concise and professional. Emotional content, such as anger, sarcasm, harsh criticism, irony, incriminating remarks and libelous references to third parties is not allowed. Employees should not expect communications they send to be private. Any material sent via YCHC's equipment is the property of YCHC. Any violations of this policy will be referred to human resources for disciplinary action.

Classification of Information for the Yakutat Community Health Center

General Public Information:
Any information that can be given to the general public and can be distributed outside of the YCHC without any risk, through the various mediums. This is often general information about the YCHC for marketing or product purposes.

Internal Information within the YCHC
Information that will not seriously impact or adversely affect YCHC if disclosed about patients, employees or business associates without proper consent or unauthorized disclosure. This may be information such as directories with phone listings, policy manuals that do not disclose PHI of individual patients and patient educational information.

Non-sensitive and/or Non-urgent PHI:
PHI that can be given by various media, (refer to YCHC's 19.0 Uses and Disclosures Policy). This information may be used internally within YCHC and received by the patient, guardian and/or authorized personal representatives (refer to YCHC Uses and Disclosures for appropriate release processes). Unauthorized disclosure could adversely impact the YCHC patients, employees and business associates. The following are examples:

- Prescription refills
- Instructions on how to take medications or apply dressings
- Appointment scheduling
- Appointment reminders
- Normal test results (other than HIV test results) with interpretation and advice
- Care and treatment recommendations
- Pre- and postoperative instructions

- Insurance and billing questions
- As a secondary means of attempting to have patients call the provider to discuss important test results and/or prognosis of a condition

Sensitive and/or Urgent Confidential PHI:
Sensitive and/or urgent confidential PHI that is intended strictly for use within YCHC and disclosed only to patients or other entities as required by law (refer to YCHC Release of Information Policy). Unauthorized disclosure could seriously and adversely impact YCHC patients, employees and business associates. Obtain an appropriate authorization for disclosures of PHI in this capacity. The following are examples:

- STD and HIV test results and/or treatment
- First means of notification for confusing or abnormal diagnostic results
- Mental health issues
- Drug and alcohol abuse and/or treatment
- Child abuse and/or neglect
- Domestic abuse
- Peer review or risk management information
- For marketing and fundraising purposes except when allowed by law (refer to YCHC 11.0 Marketing and PHI policies), and exercise caution for urgent/time sensitive matters

Procedures

The following Communication Matrix shows specific procedures in handling the various mediums of communicating information.

AUTHORIZED BY: Rhoda Jensen, Executive Health Director

CLASSIFICATION OF INFORMATION FOR YAKUTAT COMMUNITY HEALTH CENTER				
	General Public Information	**Internal Information**	**Non-sensitive and/or Non-urgent PHI** • Active measures taken to prevent the unauthorized disclosure of information from being released • If patient has notified YCHC by which means to give PHI, must be noted in their medical record and adhered to • Verification of identity must be attained in accordance with the Identity Verification Policy • Document the release in accordance with the Accounting of Disclosures Policy	**Sensitive and/or Urgent Confidential PHI** • This information may not be released without a separate signed authorization for releasing this specific information • If patient has notified YCHC by which means to give PHI, must be noted in their medical record and adhered to • Verification of identity must be attained in accordance with the Identity Verification Policy • Document the release in accordance with the Accounting of Disclosures Policy
Risk Impact	• None	• No serious or adverse affect	• Could result in adverse impact or have possible penalties applied	• Likely have a serious adverse impact. Penalties very likely to occur and could result in loss of business
1. Oral Mediums of Communication **a. Conversations** **b. Telephone** **c. Cell Phone** **d. Answering Machines** **e. Overhead Pages** **f. Lobby Announcements**	• No specific precautions	• Reasonable measures should be taken	• Conduct PHI in private settings and use lowered voices, avoiding public areas whenever possible. • If a patient name is needed, first name only basis (when possible) • Do not use a speakerphone for discussion of PHI nor retrieval of voice mail (unless in a private, closed office) • Limit discussions of PHI using a cell phone. Consider that older cell phones are not secure. • • Pages and announcements are used only to call the operator back	• Discuss PHI in a controlled manner to limit being overheard, such as in an enclosed area • If a patient name is needed, first name only basis (when possible) • Do not use a speakerphone for discussion of PHI nor retrieval of voice mail (unless in a private, closed office) • Limit discussions of PHI using a cell phone. Consider that older cell phones are not secure. • Pages and announcements are used only to call the operator back

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
2. Mail **a. Internal** **b. External**	• No specific precautions	• Information of this nature should be out of the general public areas and not accessible by anyone else, but employees	• Information being sent meets the minimum necessary requirement for disclosure • Authorized, trained personnel should handle all mail • Clearly label with recipient's name and address information is correct • Mailing item is labeled with Confidential • Tracking mechanism is recommended for external mail • Store all unattended mail in a closed, secure area • Place all types of media containing any form of PHI in secured, confidential envelopes and/or containers (internal & external) • Return address on external mail consists of YCHC name only. Envelope will not contain the department's name, provider's name (unless this is the name of the YCHC, nor the identity of the enclosed information. For tracking purposes, internal codes may be included on envelopes as long as it does not in any way relinquish the identity of the department and/or provider to anyone outside of YCHC.	• Information being sent meets the minimum necessary requirement for disclosure • Authorized, trained personnel should handle all mail • Clearly label with recipient's name and address information is correct • Mailing item is labeled with Restricted Confidential • If external, delivery of information and tracking mechanisms is required (FEDEX, messenger, certified, etc.) • Store all unattended mail in a closed, secure area • Place all types of media containing any form of PHI in secured, confidential envelopes and/or containers (internal & external) • Return address on external mail consists of YCHC's name only. Envelope will not contain the department's name, provider's name, nor the identity of the enclosed information. For tracking purposes, internal codes may be included on envelopes as long as it does not in any way relinquish the identity of the department and/or provider to anyone outside of YCHC.
3. Faxes	• Located in a secure area out of the general public • Use a coversheet	• Located in a secure area out of the general public • Use a coversheet with confidentiality	• Located in an area not accessible by the public • Coversheet with confidentiality statement used • Use reasonable efforts in dialing correct number (i.e., testing number before sending PHI), preference to	• Located in an area not accessible by the public • Coversheet with confidentiality statement used • Use reasonable efforts in dialing correct number (i.e., testing number before sending PHI), preference to

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
	with confidentiality statement • Use reasonable efforts to dial correct number • When using a means to store fax numbers, verify the number with the receiver	statement • Use reasonable efforts to dial correct number • When using a means to store fax numbers, verify the number with the receiver	using pre-programmed, labeled numbers • When using a means to store fax numbers, verify the number with the receiver • Only personnel with access to restricted area may access these faxes (review YCHC's Minimum Necessary Policy). Trained workforce member routinely checks fax machine and distributes to appropriate personnel • Faxes transmitted in error: contact person who received the fax to verify destruction of the fax and notated in patient's medical record. Report the breach to the Privacy Officer • Utilize a mechanism to ensure that the transmission went to the intended recipient (Fax logs, verification by phone, etc.) • If you receive a fax in error, immediately inform the sender and destroy the information received • Consider storing faxes in a queue until staffed	using pre-programmed, labeled numbers • When using a means to store fax numbers, verify the number with the receiver • Call prior to faxing to notify recipient of expected confidential fax • Information is immediately routed to appropriate personnel • Only personnel with access to restricted area may access these faxes (review YCHC's Minimum Necessary Policy). Trained workforce member routinely checks fax machine and distributes to authorized personnel • Faxes transmitted in error: contact person who received the fax to verify destruction of the fax and notated in patient's medical record. Report the breach to the Privacy Officer. • Utilize a mechanism to ensure that the transmission went to the intended recipient (Fax logs, verification by phone, etc.) • If you receive a fax in error, immediately inform the sender and destroy the information received • Consider storing faxes in a queue until staffed.
4. E-mail	• E-mails may be used for business purposes only • Confidentiality statement	• E-mails may be used for business purposes only • Information of this nature should be out of the general	• Prior to sending an e-mail to a patient a signed patient E-mail Informed Consent Form is received, and filed in patient's medical record. • Utilize YCHC 's secure email application at all times • 128 bit encryption [164.312(a)(2)(iv) &	• Prior to sending an e-mail to a patient a signed patient E-mail Informed Consent Form is received, and filed in patient's medical record. • Utilize YCHC's e-mail application at all times • 128 bit encryption [164.312(a)(2)(iv) &

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
E-mail Continued	attached to every e-mail • Out-of-office replies are activated during absences of more than 48 hours	public areas and not accessible by anyone else, but employees • Confidentiality statement attached to every secure e-mail • Out-of-office replies are activated during absences of more than 48 hours • If the information is time-sensitive, verify receipt of e-mail	164.312(e)(2)(ii)] • Utilize only pre-stored addresses • Verify e-mail address prior to storing the address • Use discrete, generic subject headers. Do not include the patient's name in the subject header • List sender's name, title, e-mail address, telephone number and party who patient may contact with further questions • Attach the Confidentiality statement to every e-mail • Group e-mails will only be sent in the following situations when utilizing the bcc function: impending shutdown for network maintenance, technical difficulties, recent mail blackouts, new services, change of address and/or telephone number and change in hours • If the information is time-sensitive, verify receipt of e-mail. • Workforce member routinely checks e-mails and replies to messages within 48 hours of receipt • Copy of the e-mail, including replies and receipt confirmations are filed in patient's medical records • Out-of-office replies with instructions on whom to contact for immediate assistance are activated during absences of more than 48 hours • If PHI was sent to wrong recipient, notate and document this in the patient's medical record. Report the breach to the Privacy Officer	164.312(e)(2)(ii)] • Utilize only pre-stored addresses • Verify e-mail address prior to storing the address • Use discrete, generic subject headers. Do not include the patient's name in the subject header • List sender's name, title, e-mail address, telephone number and party who patient may contact with further questions • Attach the Confidentiality statement to every e-mail • Group e-mails will only be sent in the following situations when utilizing the bcc function: impending shutdown for network maintenance, technical difficulties, recent mail blackouts, new services, change of address and/or telephone number, and change in hours • If the information is time-sensitive, verify receipt of e-mail • Workforce member routinely checks e-mails and replies to messages within 48 hours of receipt • Copy of the e-mail, including replies and receipt confirmations are filed in patient's medical records • Out-of-office replies with instructions on whom to contact for immediate assistance are activated during absences of more than 48 hours • If PHI was sent to wrong recipient, notate and document this in the patient's medical record. Report the breach to the Privacy Officer •

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
5. PDA's Personal Digital Assistant (electronic handheld device)	• No specific precautions	• Information of this nature should be out of the general public areas and not accessible by anyone else, but employees	• Password protection required, limit number of login attempts • 128 bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Antivirus software should be in place • Training to staff member with possession of PDA on situations that PDA is lost or stolen • Provide disaster recovery mechanisms • If information is not required to travel offsite or not used, then store PDA in a locked area that is out of site • Information contained in YCHC 's system may only be downloaded onto a PDA owned by YCHC, not onto a user's personal PDA	• Password protection required, limit number of login attempts • 128 bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Antivirus software should be in place • Training to staff member with possession of PDA on situations that PDA is lost or stolen • Provide disaster recovery mechanisms • If information is not required to travel offsite or not used, then store PDA in a locked area that is out of site • Information contained in YCHC's system may only be downloaded onto a PDA owned by YCHC, not onto a user's personal PDA
6. Transporting Medical Records	• No specific precautions	• Information of this nature should be out of the general public areas and not accessible by anyone else, but employees	• Utilize courier bags with a closure mechanism (i.e., Velcro, taped, tote with a lid, etc.) • Documentation (Sign out sheet or tracking sheet) for all medical records that leave the facility. Date, who took the medical record, destination location, who received the medical record and a return date, should be on this form. • Medical records are to be promptly returned upon completion of use. • Utilize YCHC's courier service whenever possible. Cab or delivery service is only used as a last resort. If cab or delivery service is used, place the medical record in a sealed envelope or container. Request the receiver to contact the sender as soon as the chart arrives at the proper destination	• Utilize courier bags with a closure mechanism (i.e., Velcro, taped, tote with a lid, etc.) • Documentation (Sign out sheet or tracking sheet) for all medical records that leave the facility. Date, who took the medical record, destination location, who received the medical record and a return date, should be on this form. • Medical records are to be promptly returned upon completion of use. • Utilize YCHC's courier service whenever possible. Cab or delivery service is only used as a last resort. If cab or delivery service is used, then place the medical record in a sealed envelope. Request the receiver to contact the sender as soon as the chart arrives at the proper destination

References

- 45 CFR 164.306
- 45 CFR 164.312(a)(2)(iv)
- 45 CFR 164.312(e)(2)(ii)
- 45 CFR 164.501
- 45 CFR 164.502
- 45 CFR 164.508
- 45 CFR 164.514 (d-f, h)
- 45 CFR 164.520(b)(1)(iii)(A)
- 45 CFR 164.522(a-b)
- 45 CFR 164.528
- 45 CFR 164.530(c)(1)

YAKUTAT COMMUNITY HEALTH CENTER

PO BOX 112
YAKUTAT, ALASKA 99689
PH: 907-784-3275 FAX: 907-784-3263

CONFIDENTIAL FACSIMILE TRANSMITTAL SHEET

To: _____ From: _____

Company: _____ Date: _____

Fax Number: _____ Number of Pages Including Cover: _____

Re: _____

_____

CONFIDENTIALITY NOTICE

DISCLOSURE STATEMENT: Protected health information is personal and sensitive information related to a person's healthcare. It is being faxed to you after appropriate authorization from the patient or under circumstances that do not require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure, and confidential manner. The authorized recipient is prohibited from using this information for purposes other than as intended. Re-disclosure without additional patient consent is prohibited, except as permitted by law. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law.

IMPORTANT NOTICE: This transmission is intended only for the use of the individual or entity to which it is addressed and may contain information that is confidential, privileged or protected. If the reader of this message is not the intended recipient, you are notified that any disclosure, distribution, or copying of this information is strictly prohibited.

CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS: Substance use disorder patient records are afforded special protections by Federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of information in this transmission that identifies a patient has having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person, unless further disclosure is expressly permitted by the written consent of the person whose information is being disclosed or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute with regard to a crime, any patient with a substance use disorder, except as otherwise provided by 42 CFR Part 2.

IF YOU HAVE RECEIVED THIS TRANSMISSION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY CALLING THE CHIEF COMPLIANCE OFFICER AT 1-907-784-3275 EXT. 123.