Coronavirus (COVID-19) Privacy FAQ

Last Updated 3/23/20

What patient information may be shared during the COVID-19 public health emergency?

- *Treatment*: Providers can use and share Protected Health Information (PHI) as needed for the treatment of a patient. Treatment is broadly defined to include direct care as well as care coordination activities. If sharing information with another individual or entity that is not subject to HIPAA (e.g. entities focusing on social determinants of health, such as Meals on Wheels), it is best to provide the patient with an opportunity to agree or object to the disclosure by simply asking them if they'd like to be referred to that entity to receive services.
- *Public Health Activities*: PHI may be disclosed for certain Public Health Activities without patient authorization. For example, PHI may be disclosed to Public Health Authorities such as the CDC, OHA or local health department as necessary to carry out their public health activities. There are other public health activities that may be permitted as well. Refer to the Use & Disclosure policy for more information or contact the Compliance & Privacy Officer or Legal department for more information.
- *Family, friends and others involved in the care of the individual*: SHS may share PHI with family members, friends and others involved in the patient's care. In light of visitor restrictions in effect system-wide, it is SHS' general philosophy that information should be shared with friends and family who request information on their loved one unless the patient objects to the disclosure, or SHS has reason to believe they may object to the disclosure. Refer to the following general guidelines that describe the potential avenues for sharing a patient's information with family and friends during this public health emergency:
    - *Opportunity to agree/object*: Where possible, workforce members should obtain verbal permission from the patient or Personal Representative prior to sharing information with friends/family or others involved in the individual's care. For requests by phone, confirm that the caller can verify the patient's identity (e.g. name, plus date of birth, phone number, address or some other identifier) prior to disclosing information. It is recommended to document the patient's agreement with sharing information with the individual in the patient's record.
    - *Friends & Family Form*: The 'Friends and Family form' is an authorization that may have been signed by the patient listing the individual(s) the patient expressly approves to receive verbal information/updates on the patient's care. This form can be found on the Documents List and/or Media tab of the patient's record. This form does not allow friends and family to receive or access the patient's medical record. Verify that the form has not been expired or revoked by the patient and ask the caller to confirm the patient's identity (e.g. name, plus date of birth, phone number, address or some other identifier) before disclosing information.
    - *Professional judgement*: If the patient is incapacitated or unable to agree or object, providers can use their professional judgement to determine, on behalf of the patient, whether the patient would object to the information being shared with the friend/family member. Refer to notes or other information in the patient's medical record as needed to determine the extent of the family member's involvement in the patient's care. When the patient becomes conscious or their Personal Representative/guardian arrives to make decisions on behalf of the patient, the

patient/representative should be given the opportunity to agree or object to continued sharing of information with friends and family. It is recommended to document these determinations in the patient's record.

- *With certain disaster relief organizations*: Limited PHI may be disclosed to disaster relief organizations such as the American Red Cross that are authorized by law or by their charters to assist in disaster relief efforts, for the purposes of coordinating the notification of family members, or other persons involved in the patient's care. Information shared for this purpose should be limited to the patient's location, general condition or death.
- *Disclosures to Prevent a Serious and Imminent Threat*: SHS may share PHI with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. SHS may disclose a patient's PHI to anyone who is in a position to prevent or lessen the serious and imminent threat, including family, friends, caregivers and law enforcement without a patient's permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety. It is recommended to document this determination in the patient's medical record.
- *Use and disclosure for Payment and Healthcare Operations*: PHI may still be used and shared for Payment and Healthcare Operations, subject to the Minimum Necessary Standard. These activities have not changed as a result of the public health emergency. See Use & Disclosure of PHI policy or contact the Compliance & Privacy Officer or Legal Department for more information.

Does HIPAA's Minimum Necessary Standard still apply to the use, disclosure, or requests for PHI during the COVID-19 public health emergency?

- Yes. HIPAA's Minimum Necessary Standard still applies to most uses and disclosures of PHI. The Minimum Necessary Standard requires SHS workforce members to only access, use, disclose and request PHI that is minimally necessary and for a permissible or required purpose (business need). Permissible uses and disclosures include those made for Payment and Healthcare Operations, and most Public Health Activities. The Minimum Necessary Standard generally does not apply to Treatment activities *so long as SHS has a current, established treatment relationship with the patient*. Instead, HIPAA defers to the provider's professional judgement in determining the amount of information necessary to treat the patient effectively.
- SHS monitors access and use of Epic and other systems to identify activities that may violate the Minimum Necessary Standard, or that may be impermissible. These monitoring activities will continue during the Covid-19 crisis. All workforce members are reminded to ensure they have a legitimate business reason to enter a patient's record, and only access the information necessary to fulfill that purpose.
- Violations of the Minimum Necessary Standard or other SHS privacy policies may result in corrective action up to and including termination.

Coronavirus (COVID-19) Privacy FAQ

Last Updated 3/23/20

What should I do if I receive a call from the media requesting information on a patient with confirmed or suspected COVID-19?

- *Facility Directory process*: In general, if the media contact asks for the patient by name, and the patient did not 'opt out' of the hospital's Facility Directory, SHS may only disclose the following information to the media contact:
    - One-word condition report (e.g. Undetermined, Fair, Serious)

  No other details about the patient – including diagnosis or contact information – should be provided, even if the information is already publicly known to the media representative or others.

- *General media requests for information on a patient with confirmed or suspected COVID-19*: Direct the request to the PR/Marketing Department who generally handles these requests. On weekends or after hours, contact nursing leadership through your chain of command or the hospital Administrator on Call.

Can I use FaceTime, Facebook Messenger Chat, Google Hangouts or similar tools to communicate with my patients and/or their family members during this public health emergency?

- Yes. The HHS Office for Civil Rights has granted an exception to HIPAA during this pandemic that allows healthcare providers to leverage these technologies to communicate with patients and their family, friends or others involved in the patient's care.
- These applications should only be used when SHS' primary audio/video technology, Microsoft Teams, fails, is incompatible with the patient or family member's device, or another means of communication is preferred.
- **Products that are public facing such as Facebook Live, Twitch, Tik Tok, and other similar applications should NOT be used to communicate with patients.**
- These tools can be used during this crisis regardless of whether the patient is receiving treatment for COVID-19.
- More information will be made available specific to Telehealth requirements, which have changed significantly in response to the COVID-19 pandemic. Refer to this HHS Office for Civil Rights Guidance for more detail.

What are my responsibilities to protect PHI and other sensitive information when working from home during this pandemic?

- Secure your physical environment by ensuring your family members cannot overhear your conversations, access your work computer or see any PHI or other sensitive information.
- Never leave your laptop, laptop bag, or other sensitive information unattended in your vehicle, even if the vehicle is locked or in your garage.
- Always use Remote Access to connect to the SHS network.
- Never use Gmail, Yahoo mail, or other personal email accounts to communicate PHI or other sensitive SHS information. Never use a personal laptop or storage device to create, use or store PHI or other SHS business information.

- Adhere to the SHS Telecommuting Policy.

What should I do if I have a question about what information I can access or share during this emergency?

- Refer to SHS policies and procedures *but note that these policies may not fully reflect the current regulatory landscape given this public health emergency.* SHS will continue to update this guidance as rules change in response to the current pandemic. Important SHS policies to reference include:
  - Use & Disclosure of PHI Policy
  - Minimum Necessary Standard policy
  - Information Privacy & Security Investigation and Corrective Action policy
  - Telecommuting Policy

- Contact anyone below with additional questions:

Compliance & Privacy	Information Security	Legal
Erick Edtl Compliance & Privacy Officer eedtl@samhealth.org Cell: 503-550-5746	James (Jim) Kelly Information Security Officer jkelly@samhealth.org Cell: 541-829-4840	Tyler Jacobsen General Counsel tjacobsen@samhealth.org Cell: 541-745-8404
Brooklyn Mills Privacy Program Manager brmills@samhealth.org Cell: 541-905-4848		Altove (Tovee) Rowly-Esch Assistant General Counsel arowley@samhealth.org Cell: 541-270-8335
Colleen Fair VP – Compliance **cfair@samhealth.org** 541-401-2951		Hanie Kim Assistant General Counsel hkim@samhealth.org 720-318-6742