## Top considerations for data privacy and security in response to our changing environment

In support of the primary mission of the hospital – 'To treat and care for patients' as well as to protect the health and safety of healthcare workers, please consider making some operational changes. These are temporary measures while navigating through these uncharted waters.

Remember: HIPAA was not meant to hinder healthcare. That is why the HIPAA Security Rule requires the implementation specification: §164.312(a)(2)(ii) Emergency access procedure.

Patient Access

- If self-check-in kiosks are available, encourage established patients to use them. Wiping down the kiosks with antimicrobial solutions in between every patient check-in may not be practical, but always have the availability of hand sanitizer at each station. Patients should be encouraged to use this before and after checking in. Also, to help reduce the spread of germs, patients could use the eraser end of a pencil or the end of a pen (acting as a stylus) rather than their finger.
  **Note:** *New or first-time patients, the* self-check-in kiosks *option may not be available to them.*
- Minimize contact with patients by offering them the opportunity to share their information (insurance card, driver's license/identification card, credit card, etc.) by taking a picture with their mobile device and…
  - Explain the risks associated with storing and sending confidential information
  - Ask them to upload their information to their account on the patient portal
    **or**
  - Send their information via a text or email
  - Remind patients that it is their responsibility to delete the photos of their personally identifiable information from their mobile device once the information has been sent
  - Remind patients that privacy is a right and a patient can give up that right at any time and often do especially in times of a dire emergency
    - Many times, a patient may have unknowingly already surrendered their right to privacy by downloading an app on their mobile device and clicking the "I agree" without reading all of the fine print
    - It is not the fault of the hospital, if there is a data breach as a result of a patient using their personally-owned mobile device which is not properly secured
  - Remind patients to periodically sanitize their mobile devices
- Have the compliance department create a scripted message for patients that can be posted on the website and/or will be used by Patient Access staff outlining the instructions for transmission and deletion of images.
- The virus could remain on their plastic cards for two to three days. By touching it, the Patient Access person may be exposing themselves.
- The more times Patient Access staff come in contact with a patient and their artifacts the greater the chances of exposure. If a Patient Access person is exposed to an individual with Corona virus, they will have to be quarantined for 14 days, thus reducing the workforce available to help with patient care. The hospital needs as many staff as possible.

Privacy and Security

- While there is some risk regarding the unsecure transmission of PHI, we believe the health benefits to patients and to hospital staff outweigh the risks. Please keep in mind that the interception of data while it is being transmitted or hacking data at rest, requires skills and tools that only some people possess.
- On March 17, the OCR stated there will be no penalties as long as the covered entity is acting in good faith.
  https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html
- Encryption for data-in-transit and at-rest are addressable implementation specifications. The use of encryption is not mandatory.
  https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html
- Maintain vigilance against hacks, scams, and phishing emails – some of the tools used by those seeking to take advantage of the crisis.

Telecommuters

Workforce members who can telecommute should be encouraged to do so. The determination of who is eligible to telecommute should be made by department managers with guidance from Human Resources and Administration. The following are some suggestions to consider for those working from home:

- Ensure that Human Resources is kept informed about plans for allowing remote workers.
  - State labor laws and union contracts may have to be assessed or exemptions granted
- Change the organization's policies regarding work from home and communicate to the workforce.
  - Consider that the virus may return again in Fall and work from home may become part of the new way of doing business in the future; plan policy changes for the long-term rather than just the immediate "shelter-in-place" situation
- Provide some type of a user agreement that the workforce must follow.
  - The agreement covers expected safeguards and controls that need to be in place
- If inbound bandwidth to the hospital's remote access infrastructure is an issue, consider staggering the hours that telecommuters work.
- Assess the number of licenses available for software supporting remote access.
- Where feasible:
  - Supply organization-owned workstations and peripheral equipment, now or at a later time
  - Implement multifactor authentication for remote workers

Telehealth

- With whole families at home and multiplying this by entire neighborhoods – bandwidth issues at the street and home level could cause problems with telehealth.
- Assess state law. In some states, the healthcare provider and the patient must both be in the same state at the time of treatment.
- Have a procedure to assess the identity of the patient and their consent prior to the start of the session. Inform patients of any possible privacy and security risks; perhaps a disclaimer stating that, while appropriate security measures have been taken, any telehealth session could be hacked.

*The intent of this document was to help you and your organization make an informed business decision. We tried to provide solutions to limiting the exposure of the virus while meeting the intent of the HIPAA Privacy and Security Rules. When in doubt, consult your legal counsel.*