HIPAA REVIEW FOR PHYSICIANS AND ALLIED HEALTH PROFESSIONALS

What is relevant to a Kaleida Health Practitioner

Introductory

This review addresses the requirements of the Privacy and Security rules under the Health Insurance and Portability and Accountability Act of 1996 (HIPAA).

While reference is mainly made to the Privacy provisions, the Privacy and Security rules work in tandem in strengthening patient rights and privacy protections. The regulations boil down to 1) for the practitioner – more responsibility to protect the patient's privacy, and 2) for the patient – more control.

<u>Primary</u> reasons we comply with these requirements:

- *It's the law*
- *HIPAA supports our institution's commitment to respect patient privacy and confidentiality*
- *Privacy violation complaints can jeopardize the hard earned reputation and respect of the institution and the individual practitioner*
- *It is part of the good care and services we provide our patients*

<u>Secondary</u> reasons we comply with these requirements:

- *Patients can file complaints directly with the Department of Health and Human Services (HHS)Office for Civil Rights (OCR)*
- *Violations are subject to both civil and criminal penalties*

What are we protecting, and how?

Protected Health Information (PHI), which is any information about a patient that we (Kaleida Health) create or collect which can be linked back to an individual.

We protect PHI from uses (internal) or disclosures (external) that are not authorized by the patient or are not for appropriate use in treatment, payment or Kaleida Health operations.

Internally we must use PHI only to conduct the duties for which we are responsible. This is why only certain individuals have access to PHI and the level of access is controlled to minimize the ability to see certain PHI. This is what is called Minimum Necessary and Need-to-Know. This also applies to access in restricted areas of the hospital. Minimum Necessary also impacts:

- Looking only at the PHI of the patients for which you are involved in treating
- Do not look at your own PHI, your family member or a friend, unless you are participating in the care of this individual.
- Even when sharing information for treatment or payment purposes make sure it is only what is necessary and appropriate.

Safeguards

Safeguarding PHI can be time consuming and costly. For this reason, the regulations refer to **reasonable** measures for protection of PHI. Here are a few tips:

- Although being overheard by others when talking to patients/family members in non-private rooms, small waiting areas or other areas can be considered an *incidental disclosure (this is a permissible type of disclosure under the regulation),* we must make every effort to:
    - Speak softly
    - Move to an area of the room where the most privacy is available
    - Use private rooms to communicate with family or patients, when available
    - Ask the family or patient if they feel comfortable discussing this information at the current location you have chosen
- Close and lock doors of/leading to rooms that hold PHI
- Do not leave documents with PHI where they can be accessed by others
- Do not discuss PHI in public areas (e.g., hallways, elevators, etc.)
- Keep your laptop or personal digital assistant (PDA) secure and with passwords.
- Dispose of documents with PHI by shredding or placing it in a locked and confidential document destruction bin.
- Do not share your computer password or access to restricted area with anyone under any circumstances

Patient Rights

Accounting of Disclosures

- Patients can request a list of the individuals/entities to which you disclosed their information. This means that you or your staff will have to log and track the disclosures you make to external entities for purposes other than treatment, payment or certain healthcare operations and for which no patient authorization was obtained.

Access to Medical Records

- Although patients have always had this right, HIPAA enforces their ability to access the record in a timely manner.

Request to Amend Medical Record

- Patients can request in writing to have their medical record amended if they feel the information is incorrect. The practitioner responsible for the information in question determines if in fact a correction is or is not required. Even if the change is not made, a copy of the request is kept in the medical record.

Facility Directory

- A patient can choose to be excluded from the facility directory. The patient will appear to anyone calling or stopping by, as if she/he were not at our facility. A patient who is not excluded and therefore part of our directory can be reached by someone asking for

her/him by full name. We can then provider patient location and general condition of the patient.

Family/Friend Involvement

- The patient chooses whom we can and cannot communicate with regarding their care. At Kaleida Health we ask the patient to provide one or two names that we can share information with. This person(s) then becomes our point of contract and we direct anyone else asking detailed information about the patient to the person(s).

Alternate Means of Communications and Restrictions to Use and Disclose PHI

- A patient can request to be contacted via an alternate route (e.g., number, different address, cell phone, etc.) The patient can also request that their information not be used or disclosed in a certain way. These requests must be evaluated individually to verify that Kaleida Health can assure 100% compliance before it is agreed to.

File a Complaint

- Patients can file a complaint regarding their privacy directly with the US Department of Health and Human Services Office for Civil Rights. That information is provided to them in our Notice of Privacy Practices or they can contact the Kaleida Health Chief Compliance Officer to file their complaint.

IS&T Security Alert on Protected Health Information

Protected Health Information (PHI)

Social Media:

- Kaleida Health workforce members may not use or disclose any member/patient identifiable information of any kind on any social media. Even if an individual is not identified by name within the information you wish to use or disclose, if there is a reasonable basis to believe that the person could still be identified from that information, then its use or disclosure could constitute a violation of the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and Kaleida Health policy. (IS.05 Internet Access Policy)

Text Messaging:

- PHI should never be sent in a text message unless you can guarantee the text is communicated from the sending device, though the mobile provider(s) to the recipient's device in an encrypted manner.

- Protecting Mobile Devices:
  - Use a password or other user authentication
  - Do not store PHI or sensitive information on the device
  - Install and enable encryption
  - Install and activate remote wiping and/or remote disabling
  - Disable and do not install or use file sharing applications
  - Delete all stored health information before discarding or reusing the mobile device

- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes.

Contact Information

For Privacy related questions, please contact Robert Trusiak, Chief Compliance Officer/Privacy Officer, at (716) 859-8053 or (716) 352-0196 or by e-mail at RTrusiak@kaleidahealth.org. For Information Security related questions, please contact Tom McDonald, Information Security Officer, at 859-8126 or by e-mail at TMcdonald@kaleidahealth.org.