Helpful Hints on Top Things Every Privacy Officer Needs to Know But Won't Encounter Every Day

Presented by:

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC

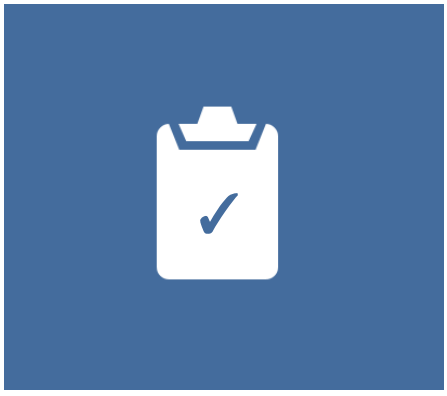
Vice President of Audit Strategy

CYNERGISTEK

CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

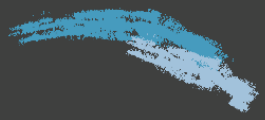
CynergisTek has been recognized by KLAS in the 2016 and 2018 Cybersecurity report as a top performing firm in healthcare cybersecurity.

Today's Agenda



1. ROI – Minors, law enforcement, etc.
2. Business Associate Agreements
3. Marketing, Fundraising & Research
4. Phones, Photos & Privacy
5. Questions

ROI - Minors, Law Enforcement, etc.



Release of Information Regarding Minors

- Understanding the Rule
  - Parent/Guardian or other stands in the shoes of the child except when they don't
  - Don't confuse sharing with family and friends with a personal representative
  - State law nuances
    - Minor rights
    - Emancipated minors
    - Divorced parents

Release of Information Regarding Minors

- Make practical decisions
  - Patient portal access
  - HIE
  - Care EveryWhere

Law Enforcement

- All HIPAA disclosures of information for law enforcement are permissive.
- Six exceptions under 45 C.F.R. 164.512(f)
  - Pursuant to process or required by law
  - Identification & location
  - Victims of a crime
  - Decedents
  - Crime on the premises
  - Reporting a crime in an emergency

Law Enforcement - Pursuant to Process

- Proactive - under legal obligations
- Reactive – Court order, warrant, subpoena or summons issued by a **judicial officer**, grand jury subpoena, subpoena with reasonable assurances

Law Enforcement - Identification and Location

- Reactive – subject to law enforcement request
- Limitations on what can be disclosed
- Cannot disclose
  - DNA or DNA analysis
  - Dental records
  - Typing, sampling or analysis of bodily fluids or tissue

Law Enforcement - Victims of a Crime

- Reactive – subject to law enforcement request
- About an individual who is or is suspected to be a victim of a crime
  - Individual must agree to the disclosure or
  - If unable to obtain the individual's agreement because of incapacity or emergent condition IF
    - LOE represents the PHI is needed to determine a violation of the law by someone other than the patient and the information will not be used against the patient and
    - There is an immediate law enforcement need that will be materially and adversely affected without disclosure and
    - The CE determines it is in the best interest of the patient

Law Enforcement - Decedents

- Proactive – CE can disclose information about a deceased patient to alert the LOE that the death is suspected to be the result of criminal conduct.

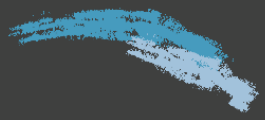
Law Enforcement - Crime on the Premises

- Proactive – CE can disclose PHI to LOE if the CE believes in good faith that the information constitutes evidence of criminal conduct that occurred on the CE's premise.

Law Enforcement - Reporting a Crime in an Emergency

- A CE providing emergency medical care in response to a medical emergency, not on the CE's premises, may disclose PHI to a LOE if the disclosure appears necessary to alert the LOE of:
  - Commission and nature of a crime
  - Location of the crime or the victim and
  - Identification, description and location of perpetrators of the crime
- However, if the CE believes the medical emergency is the result of abuse, neglect or domestic violence this exception does not apply and 164.512(c) must be followed.

Business Associate Agreements



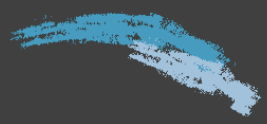
Key Terms to Reconsider

- Notification of security incidents
  - What does your BAA say?
  - Definition of a security incident
- Notification of a breach
  - What does your BAA say?
    - Time for notification
      - Regulations
      - State law
    - Definition of a breach
  - Do you want you BA determining if a data compromise is a breach?

Key Terms to Reconsider

- Process for reasonable assurances
  - Ongoing assessments
    - Reputable 3rd party reviews
- Status of data at termination of the agreement.
  - Do they get to keep it?
  - How are you assured they are continuing to protect it?
  - Have you considered minimal necessary?

Marketing, Fundraising and Research



Issues with Marketing

- Remember the definition of marketing
  - Not marketing is marketing when remuneration is received
    - Communications for treatment or alternative treatments
    - Description of health related product or service provided by or included in a plan of benefits
- Who decides what is not marketing?
- Sale of PHI
  - Always requires authorization

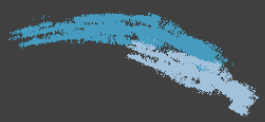
Issues with Fundraising

- What fundraising is occurring in your organization?
  - Close relationships with associations
  - Physician lecture
- Does everyone understand what an institutionally related foundation is?
- Is your NPP updated?

Issues with Research

- This has always been a complex area
  - Nature of of the organization
  - Nature of the relationship between organizations
- How does the data exist in the EHR?
- Is your NPP being provided to patients?
- Waivers of authorization
  - Confidence in the IRB or Privacy Board
  - Audits of the process

Phones, Photos & Privacy



Use of Cell Phones in Healthcare

- BYOD
- Emails
- Text/IM
- Photos/Videos
- Apps on the phone
- Patient phones

BYOD - You can't stop it!

- Unlikely a covered entity can avoid all issues with BYOD
- What is the policy on the use of personal devices?
- Have you educated your workforce on
  - How information is stored and backed up on their phone
  - Whether the use is appropriate or not

Emails

- Can users get their work email on a personal device?
  - What protections do you have in place if the answer is yes
    - Is it secure?
    - What happens when the user leaves the organization?
    - Can users forward their email to a personal account?
    - What is the back-up on the personal device?
    - What about patient communications?
- Can personal email be used for work?

Texting and Instant Messaging

- Are users permitted to text or IM PHI?
  - How much?
- Do you have a secure texting/IM solution?
- CMS guidance on secure texting
- What is if it is on a personal phone?

Photos and Videos

- Can a user take photos or videos on a personal device?
  - If so under what circumstances?
  - What happens to the photo or video once it is taken?
    - Should it be transferred to the EHR?

Apps on the Phone

- Can clinicians use apps on their phone for patient care?
  - Apps that calculate information on the patient
  - Apps that record patient information
  - Dictation apps

Patient Phones

- Do you have a policy addressing patient phones?
  - What they can photographs?
  - What they can record?
  - Where can they take cell phones in your facility?
  - Can a care provider record information on a patient phone?

Thank You!

Marti Arvin
Executive Advisor
marti.arvin@cynergistek.com
512.450.8550 x7051