WORKSHOP IV

Integrating Ethics, Compliance, Privacy and Security into a Single Organizational Initiative

Geralyn Kidera JD

Senior Vice President
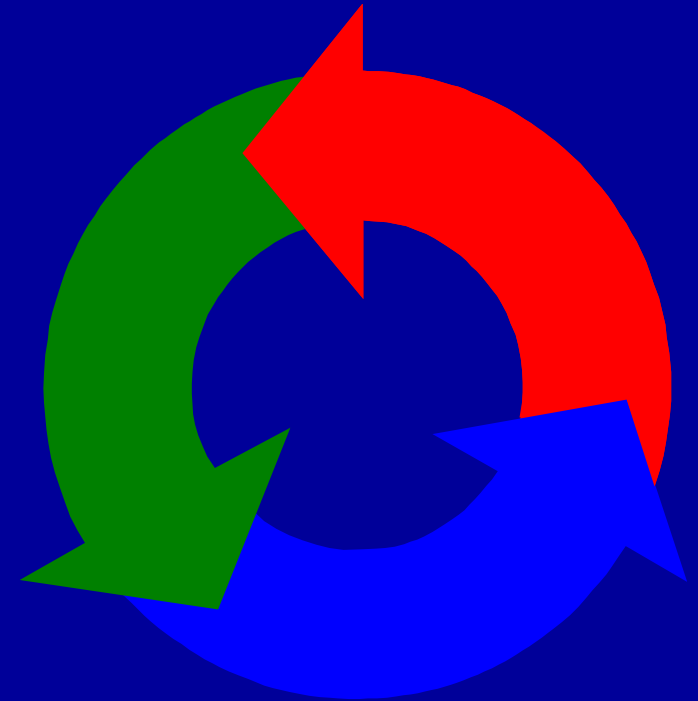
Council of Ethical Organizations/Health Ethics Trust

Discussion Point

- What are your expectations for this workshop?
- What would you like to learn, discuss, share?

What Do Ethics, Compliance, Privacy and Security Have To Do With Each Other?

- 1. The role of ethics in compliance
  - > going beyond the 'rules'
  - > focusing on shared values
  - > rewarding ethical decision-making

- 2.   Privacy - a fundamental concept in healthcare
  - > values-driven or rule driven?
  - > Patient focused or provider/payer focused?
  - > Why now?

- 3. Security - how does this relate to our compliance program?
  - \> IT's problem?
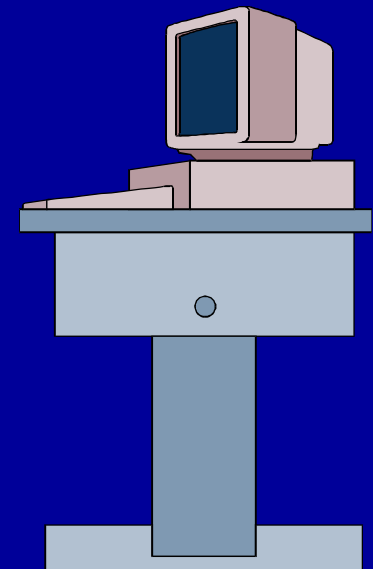
Case Study

- In a small physician office, the nurse sits behind the window in the back of the patient waiting area. The window is open so that she can easily talk with patients as they come in for their appointments. One of her responsibilities is to call patients to remind them of appointments, or to discuss the results of blood tests or x-rays taken when the patient was the office.

- She calls a patient to discuss the need to schedule additional visits to the physician's office as a result of some preliminary tests that were taken. When she calls the patient she calls her by name (to verify she is indeed speaking with the patient) and proceeds to discuss the test results.

- Several patients sit in the waiting area. They can hear the nurse's side of the telephone conversation.

- Are there any privacy compliance issues here? How do you address the ethical issues?

- What is the appropriate way for the nurse to do her job?

Discussion Point

- A. How did your organization develop its compliance program?
    - Who was involved?
    - Who drove the process?
    - Who ended up as CCO….and why?

- B. What is your organization's approach to implementing a HIPAA privacy and/or security initiative?

Elements of a Single Initiative

- 1. What is role of compliance/integrity program?
    - Setting expectations
    - Defining organizational values
    - Providing tools to enable employees to meet expectations within those values
    - Prevent and deter wrongdoing
    - Respond promptly and responsibly to problems
    - → Internally driven initiative?

- 2. How do your privacy and security initiatives impact compliance efforts?
  - Setting expectations
  - Defining organizational values
  - Providing tools
  - Responding to problems
  - → Externally driven mandate?

- 3. How does "ethics" help to shape that initiative?
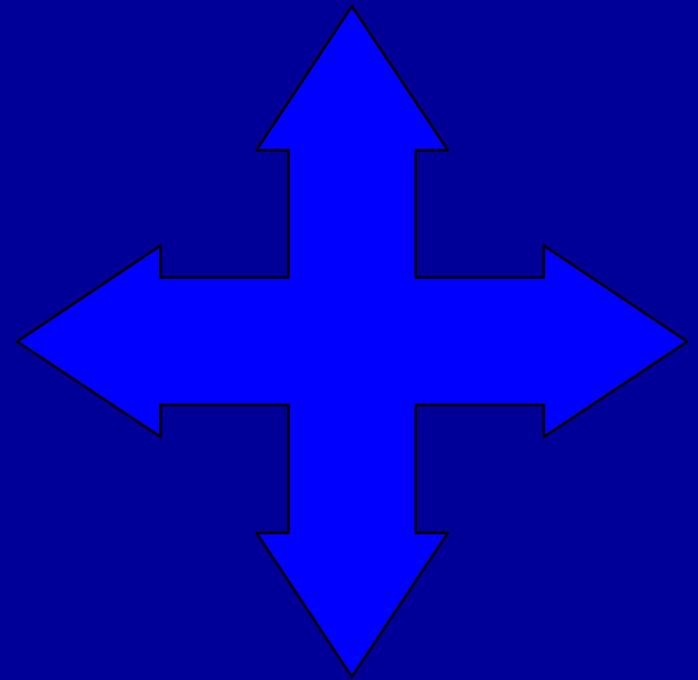
Discussion Point

- How do you resolve conflicts between operational needs and organizational values?

- How do you demonstrate your organization's values through systems, protocols, processes?

Role of Compliance Officer

- 1. Should CCO also assume role of Privacy Officer?
    - > compatible goals
    - > wide area of responsibilities
    - > high level position?
    - > clearly defined role(s)?

Policies & Procedures

- 1. Privacy -
    - > driven by regulatory requirements (and state law)
    - > reconciling patient needs and operational concerns
    - > need for 'team' to create/implement
    - > who 'owns' them?

- 2. Security
    - > technical component - requires IT input
    - > equipment needs - dictate process
    - > human element - protocols to be followed
    - > transaction issues - driven by government/payer requirements

Case Study

- A number of physicians on staff at the hospital are able to access the hospital electronic medical record system from their medical offices. This allows them to review test results and other information concerning their patients and provide immediate information concerning treatment changes to the hospital staff. One of the physicians wishes to have the same remote access from his home office, so that he can check on his patients when he is at home. He has a computer and high speed internet access and wants to be able to access the hospital system whenever he can.

- His computer is located in his den at home. While his kids do occasionally use the computer, he assures the hospital that only he will ever access the hospital's records.

- What are the hospital's obligations here?

- What are the doctor's responsibilities?

- How do you view this issue from an ethical/values-driven basis?

Privacy/security and Your Reporting Process

- Are you prepared to address hotline calls (or other reports) concerning privacy and/or security issues?

  > What procedures are in place?

  > Who conducts investigation and follow up?

Training

- Privacy training of 'workforce' - how will that be accomplished?
    > Who will conduct it?
    > How will it be given?
    > Who will be required to attend?

- What will be your 'message'?
  - > Will it incorporate your organization's shared & stated values?
  - > How will you articulate them?

- What about security training?
  - > How do you make sure your organization's security protocols are understood and followed?
  - > Who needs to be trained? Why?

- What about your compliance training efforts? Do they get lost or put on hold?
  - > How do you deal with limited resources and multiple priorities?
  - > Are these efforts mutually exclusive?

Case Study

- *A large physician group practice is struggling with its HIPAA compliance program implementation. The practice has decided to use new computer software and terminals to manage access to archived and ongoing healthcare information about its patients. The practice has decided that all physicians will have to learn how to use the computer terminals in order to view lab and other test results, and to review patient histories. The practice manager knows that he will not be able to convince all of the physicians to adopt a totally electronic medical record, but believes these changes are a good first step into the use of electronic data management, and in achieving compliance with HIPAA requirements. In addition, the practice's IT department believes that the new technologies will result in more efficient use of physician and staff time, assure secure data collection and storage and allow the practice to monitor access to all protected health information.*

- *Most of the staff is very supportive and enthusiastic about the new system enhancements. However there are several older physicians who aren't interested in learning about compute or how to use them in their own practice. They have been totally resistant to taking any time to learn about the electronic data system, or the use of any "new-fangled" stuff.*

- *Several of the physicians have told their own staff members to "take care of this stuff" for them, and believe that will be sufficient to meet any requirements. The physicians understand that HIPAA will apply to the group practice; however, they believe things would be a whole lot simpler if the practice didn't get into use of computers and other electronic data processes. They are very vocal in complaining about having to take staff time (not to mention their own time away from patients) to learn about the new systems.*

- *Can the practice rely on training the physicians' staff members?*
- *How do you deal with physicians who resist any training programs?*
- *How do you incorporate shared values into hard-subject training like this?*