

Training Clinical Research Professionals

**Prepared by the
NCHICA Research Work Group
Privacy and Confidentiality Focus Group**

**Approved for Public Distribution
November 13, 2001**

Introduction

It is difficult to refute that information technology has improved many aspects of healthcare. However, these benefits stand amidst much trepidation related to the privacy and security of personal health information. In response to these concerns, regulations have been introduced which impose strict rules upon individuals who manage individually identifiable data. One such rule deals with the need to educate clinical investigators about data privacy. This report is aimed at providing recommendations for the development of privacy training modules for clinical research professionals.

Computer-Based Patient Record Institute (CPRI) Model

Background

Computer-based Patient Record Institute (CPRI) is dedicated to advancing improvements in health care quality, cost, and access via the regular use of information technology. CPRI serves as a neutral environment for bringing different interests of health care stakeholders together to create shared solutions. Some of CPRI's members include 3M Health Information Systems, American Academy of Family Physicians, American Board of Family Practice, American College of Physicians, American Hospital Association, Association of Operating Room Nurses, Ernst & Young, and the Mayo Foundation.

When organizations require personnel to abide by rigorous policies, procedures, and practices for preserving confidentiality, these organizations also take on the responsibility for providing initial and continuing education. To this end, CPRI recommends that health care organizations adopt a regular, mandatory educational program as well as an annual refresher program to continue to inform staff about matters related to security and confidentiality of patient data.

CPRI Toolkit: Managing Information Security in Health Care, Version 2 is a resource developed by CPRI to facilitate the creation, implementation, and evaluation of an organization's information security education program. While the CPRI model specifically addresses training related to health care security it should be noted that much of this also applies to privacy training. The CPRI model may be accessed via the following link: http://www.cpri-host.org/toolkit/4_6_1.html.

Training Investigators: Special Considerations

Challenges may emerge while providing investigators and staff privacy and data privacy training. However, these barriers can be curtailed through preparation and a specially designed educational program. Before planning a program for physicians, the following section should be considered.

Numerous challenges to effectively training medical staff on data privacy and security issues have been posed. These include:

- The hectic schedules that most physicians have;
- The various relationships between medical centers and physicians: a physician might be directly employed by a medical center, work on a contractual basis, or may simply hold admitting privileges;
- Historically, medical staff has not been required to attend training; and

Copyright (c) 2001 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/default.asp> and which is available from NCHICA upon request.

- “Physicians often view training as a disruptive and unnecessary intrusion into an already busy schedule with competing demands.”¹

Developing A Privacy Awareness Course: Considerations

The HIPAA law provides minimal guidance on the development and implementation of privacy training. The following represents considerations that should be made by individuals and groups developing a privacy program.

Training Structure and Logistics

- The development of a training task force is often necessary. This group should include employees who have an array of specialties and represent the entity’s different lines of business. Including at least one physician on the task force is helpful in receiving medical staff support with the course.
- Develop a timeline consistent with the HIPAA compliance date.
- Who is the audience? How large is the audience?
- Coordinate the terms, policies, and procedures for the audience with other audiences at the same institution (e.g. nurses, allied health, administrators).
- What is the most ideal way to disseminate training to participants? For instance live presentations, conference call, or self-guided instruction.
- Will participants benefit from an accompanying PowerPoint presentation?
- It may be necessary to develop multiple levels of training (i.e. basic and advanced training, or specialized to staff responsibilities.)
- Prioritize the course rollout based on the amount of protected health information handled by various units / lines of business.
- How will participants be notified of scheduled classes or course completion status?

Content

- Consider informing participants that privacy training is mandatory for covered entities under HIPAA. (This is highly suggested, as some participants may express dissatisfaction because they view this course as too basic or perhaps unrelated to their position within the organization.)
- In addition to an overview of HIPAA, entities engaged in international transactions should consider incorporating an overview of the European Union Data Protection Directive.
- It is crucial to include privacy violation scenarios specific to the entity’s use of protected health information.
- Employees should be informed of the entity’s practices, policies, and procedures for the protection of individually identifiable health information. Contact information for the organization’s Privacy Complaint Office point of contact and Privacy Officer should also be provided.
- Inform participants whom they may contact if they have questions after the presentation.

¹ “Organizational Approaches to Protecting Electronic Health Information,” *For The Record: Protecting Electronic Health Information* at <http://www.nap.edu/readingroom/books/for/5.html>

Evaluation

Participants' level of comprehension should be assessed post presentation, But, before deciding what type of an evaluation tool best suits an organization, the following should be considered:

- Archiving the evaluation document: what archiving format will best meet the needs of the organization? For instance, is it easier and or more efficient to maintain the record of completion in an electronic format as opposed to a paper format?
- If a post presentation quiz is used: what will constitute a passing score, what is the policy related to participants who do not pass the quiz, and who will grade the quizzes?