

**- NCHICA -**

***A State Collaboration to Develop  
Tools Including Gap Analysis  
Programs to Cope with HIPAA***

***Presented to the 2002 CMS HIPAA/MMIS Conference***

***Hunt Valley, Maryland***

***April 22, 2002***

***Holt Anderson, Executive Director, NCHICA***

# WHAT IS NCHICA ?

- 501(c)(3) nonprofit research & education
- Established in 1994
- 250+ members including:
  - Providers
  - Health Plans
  - Clearinghouses
  - **State & Federal Government Agencies**
  - Professional Associations and Societies
  - Research & Pharmaceutical Research Organizations
  - Vendors
- Mission: Implement information technology and secure communications in healthcare

# *State Agencies Participating From:*

- **AK**
- **KY**
- **LA**
- **NC**
- **NM**
- **NY**
- **OK**
- **SC**
- **UT**

# **NCHICA HIPAA Implementation Planning Task Force** (Established 1999)

- **Goal:**
  - Develop overall strategy for addressing HIPAA compliance in an orderly and most efficient manner possible.
- **Work Groups:**
  - Transactions, Codes & Identifiers
  - Data Security
  - Network Security & Interoperability
  - Privacy
  - Awareness, Education & Training
- **300+ Participants Involved**

# HIPAA Implementation Planning Task Force

Dave Kirby (Duke Univ. Health Sys), Harry Reynolds (BCBS)

## Transactions, Codes and Identifiers

Stacey Barber (EDS)  
Roger McKinney (Carolinas Health System)  
Ken Pervine (Bladen County Hospital)  
Jim Walsh (UNC Hospitals)

## Awareness, Education and Training

Steve Wagner (NC MGMA)  
Katherine McGinnis (Eastern AHEC)  
Stephanie Simon (BCBSNC)

## Privacy

Jean Foster (Pitt Co Mem. Hosp.)  
Judy Beach (Quintiles)

## Security

Dave McKelvey (Duke Univ.)  
Joe Christopher (Sampson Regional MC)  
Harold Frohman (Raytheon)  
Rosemary Abell (Keane)

## Consent & Patient Rights

### Contracts

### Minimum Necessary Disclosure

### Minors' Issues

### Research

### State Law

## Network Security & Interoperability

### Data Security

# Deliverables

- Awareness and Educational Sessions
- Workshops
- Training Materials
- White Papers
- Preemption Analysis
- Sample Documents
- Gap Analysis & Planning Tools

# A Comment About Tools

- HIPAA Complexity has driven the need for tools to help manage compliance planning
- There are a growing number of responses to choose from, both paper and computer-based
- Capabilities and costs vary greatly

# Tools Include:

- HIPAADocs
- HIPAATRAAC from HealthLink
- HOST-CPRI Toolkit
- Meridian Health System (NJ) tool
- RiskDoctor from Raytheon
- RiskWatch
- TriZetto
- Utah Security Education Tool (USET)
- Others ...



# Self-assessment / Gap Analysis Tools

*HIPAA EarlyView™ Security*

*HIPAA EarlyView™ Privacy*

# Uses of *HIPAA EarlyView*<sup>TM</sup>

- Staff education
- Gap analysis
  - Inadequate or missing policies
  - Previously unidentified vulnerabilities
- Data to begin budget planning process
- Due diligence documentation



# ***Security***

## **A Tool for Security Gap Analysis**

© 2000 North Carolina Healthcare Information & Communications Alliance, Inc.  
(NCHICA)

# Security Questions

This form is used by a facilitator to conduct the HIPAA Security Questionnaire. It is designed to be used to capture all required information. Comments should be forwarded to DataSecurity@NCHICA.ORG. Thanks!

Question **1**

Questionnaire Name: sample1

**Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?**

Answer:  Yes  No  N/A  Unanswered

Due Diligence Demonstrated:  Check if YES

Comments: evaluation done by test org - june 1999

Refer To:

Document Name: tech eval

Doc Type: Paper Document Location:

Periodically Reviewed? No Next Review Date (MM/DD/YYYY):

Point of Contact: Mr. Contact Contact Phone: (999) 999-9999 Ext. 1234

Contact Title: boss Contact E-Mail: boss@sample.com

Contact FAX: (999) 999-9999

Answer Date (M/D/Y): 6/9/00

Readdress Requirement:

# Report Example

## Questions answered with "NO"

sample1

HIPAA Table

A

HIPAA Requirement Certification

HIPAA Implementation

Question Number	Detailed Question	Refer To:	Contact	Contact Phone
2	Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?	Susan Reference		



# *HIPAA EarlyView™ – Privacy*

Target your weaknesses with this powerful self-evaluation tool

## ***Privacy***

A Tool for Privacy Gap Analysis and  
Documentation

# ***HIPAA EarlyView™ Privacy***

## Developed by:

- The Maryland Health Care Commission (MHCC)
- The North Carolina Healthcare Information & Communications Alliance, Inc. (NCHICA)

# Highlights

- 33 Requirements from the Privacy Rule
- 43 Questions keyed to Requirements
- Incorporates industry “best practices”
- Includes recommended “action items” to fulfill each Requirement
- Links to online sample documents, document portfolio management facility
- User Guide

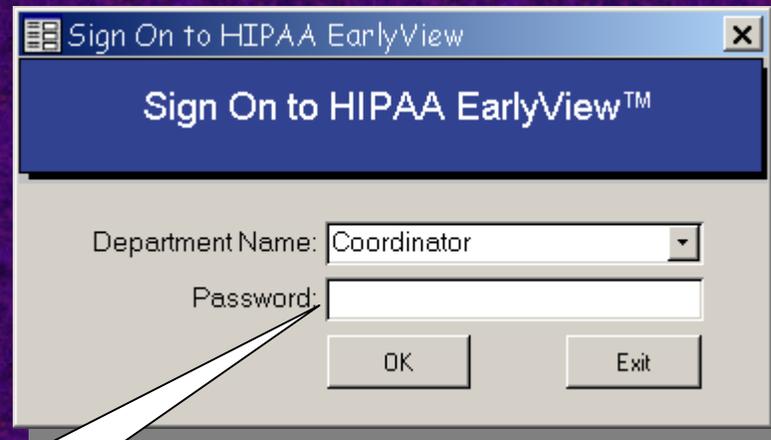
# What does HEVp Do?

- *Organizes* your initiative toward compliance with HIPAA privacy rules
- Provides a '*gap analysis*' to show what you need to do to comply
- *Clarifies* the HIPAA privacy regulations
- Provides a program of *action* for HIPAA compliance
- Provides *templates* for key HIPAA documents

**Tour of**  
***HIPAA EarlyView™ Privacy***

# Login

The Coordinator can configure HEVp for multiple users & departments. Initially, the Coordinator is the only user.



Sign On to HIPAA EarlyView

Sign On to HIPAA EarlyView™

Department Name: Coordinator

Password:

OK Exit

The Coordinator password is initially blank

# Main Menu

Provides access to all HEV features

Help is available for most functions.

The screenshot shows a web application window titled "Main Menu". The main content area has a dark blue header with the text "HIPAA EarlyView™ Privacy". Below the header, there is a form with the following elements:

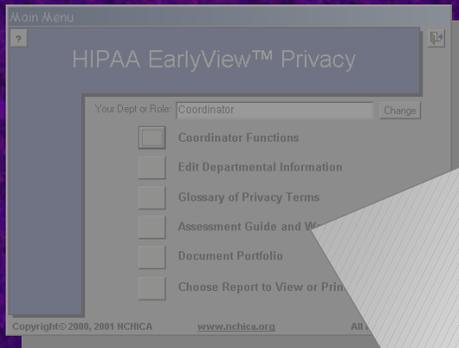
- A label "Your Dept or Role:" followed by a text input field containing "Coordinator" and a "Change" button.
- A list of menu items, each with a square button to its left:
  - Coordinator Functions**
  - Edit Departmental Information**
  - Glossary of Privacy Terms**
  - Assessment Guide and Work Plan**
  - Document Portfolio**
  - Choose Report to View or Print**

At the bottom of the window, there is a footer with the following text:

Copyright© 2000, 2001 NCHICA      [www.nchica.org](http://www.nchica.org)      All Rights Reserved

# Assessment Guide and Work Plan

For each requirement: clarification, assessment, action items



Requirement

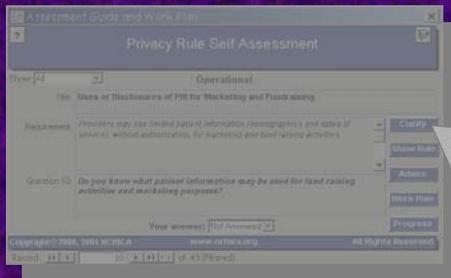
The main application window is titled 'Assessment Guide and Work Plan' and 'Privacy Rule Self Assessment'. It displays a list of requirements. The selected requirement is 'Operational' with the title 'Uses or Disclosures of PHI for Marketing and Fundraising'. The requirement text is: 'Providers may use limited patient information (demographics and dates of service), without authorization, for marketing and fund raising activities.' Below this is 'Question 10: Do you know what patient information may be used for fund raising activities and marketing purposes?'. The 'Your answer:' field is set to 'Not Answered'. On the right side, there are buttons for 'Clarify', 'Show Rule', 'Advice', 'Work Plan', and 'Progress'. The footer shows 'Copyright© 2000, 2001 NCHICA www.nchica.org All Rights Reserved' and 'of 43 (Filtered)'.

Assessment question

Response to question

# Requirement Clarification

Provides expanded discussion of each requirement



## Clarification

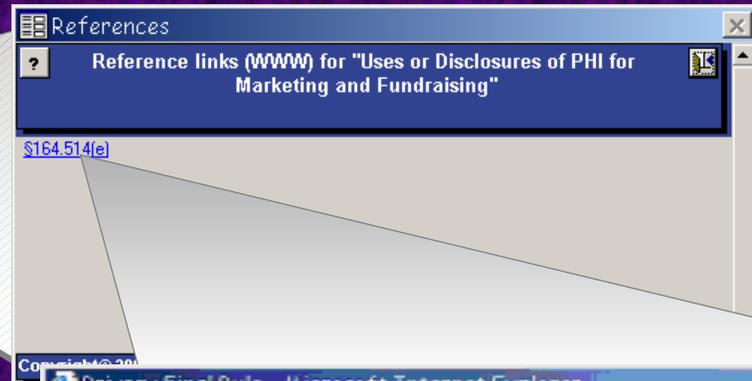
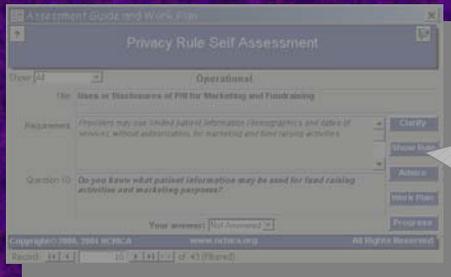
Uses or Disclosures of PHI for Marketing and Fundraising

Except for general communications (i.e., newsletters), disclosures for marketing and fund raising must notify individuals on how their name may be removed from receiving future solicitations.

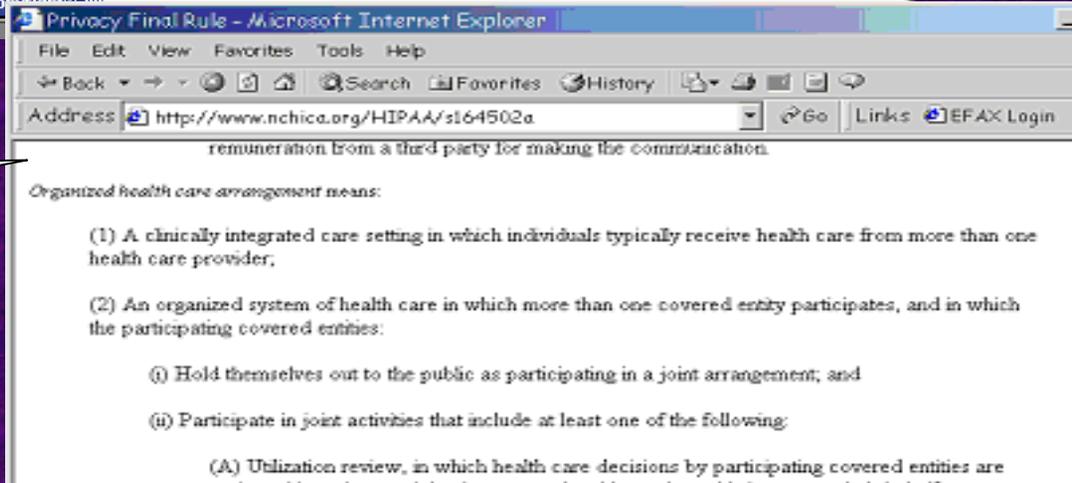
OK

# Rule Text

Shows actual text of the Privacy rule for each requirement



Rule text linked from NCHICA's web site



- remuneration from a third party for making the communication.
- Organized health care arrangement means:
- (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
  - (2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
    - (i) Hold themselves out to the public as participating in a joint arrangement; and
    - (ii) Participate in joint activities that include at least one of the following:
      - (A) Utilization review, in which health care decisions by participating covered entities are

# Best Practices Advice

Provides advice from industry experts on how to comply with a requirement

Assessment guide and Work Plan

## Privacy Rule Self Assessment

Operational

Uses or Disclosures of PHI for Marketing and Fundraising

Requirement: Providers may not include patient information (demographics and dates of services) without authorization for marketing and fund raising activities.

Question: Do you know what patient information may be used for fund raising activities and marketing purposes?

Your answer: Not Answered

Copyright 2009, 2011 HHS/ONC www.hhs.gov All Rights Reserved

## Best Practice

Uses or Disclosures of PHI for Marketing and Fundraising

Inform individuals of the right to opt-out of marketing and fund raising communications as part of patient registration by including a statement of choice.

Include the organization's marketing and fund raising policy in the Notice of Privacy Practices. Identify marketing practices pertaining to face-to-face encounters and products with nominal value.

Review Health Information System to determine if patient records can be flagged for individuals that opt-out of marketing and fundraising communications.

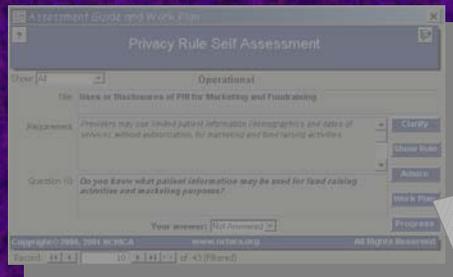
OK

# Work Plan

Each requirement has a set of action items for compliance.

Expanded description of suggested action

Documents required for compliance

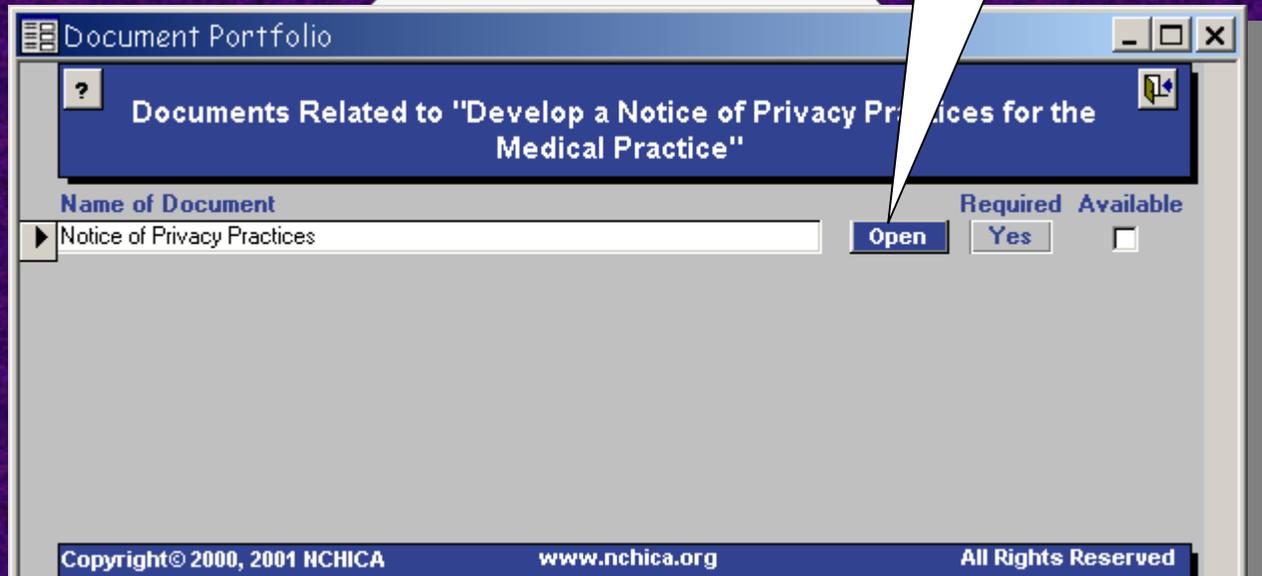
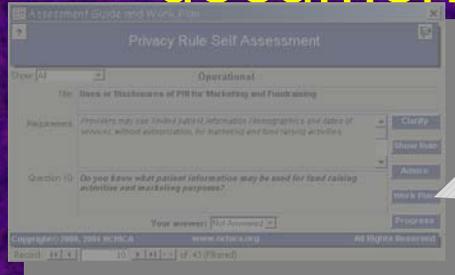


A screenshot of the 'Recommended Actions' section in the Privacy Rule Self Assessment tool. The title is 'Action Items for "Uses or Disclosures of PHI for Marketing and Fundraising"'. It lists two action items, each with an 'Explain' button and a 'Documents' button. The first action item is 'Develop a Notice of Privacy Practices for the Medical Practice' and the second is 'Develop and implement a training program for all employees'. Both 'Documents' buttons have a 'Completed' checkbox next to them. The footer contains copyright information for NCHICA and a record count of 1 of 2 (Filtered).

# Compliance Documents

Actions frequently require preparation of a document.

Link to document or template



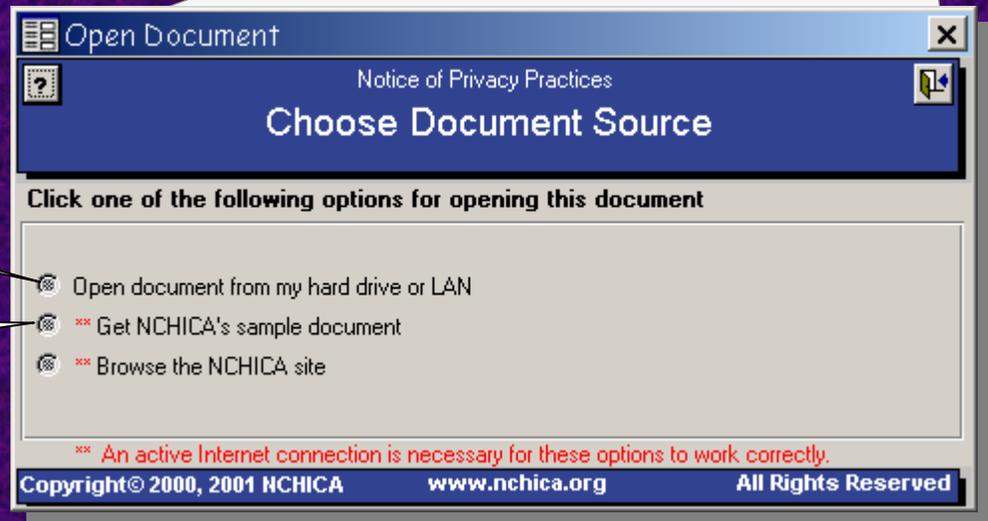
# Document Management

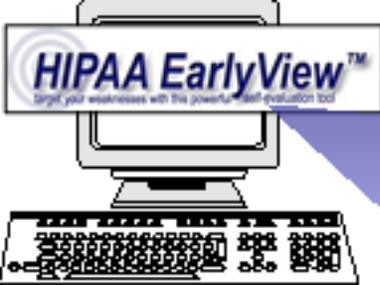
You can create and manage your organization's compliance documents.



Link to local document

Link to on-line template





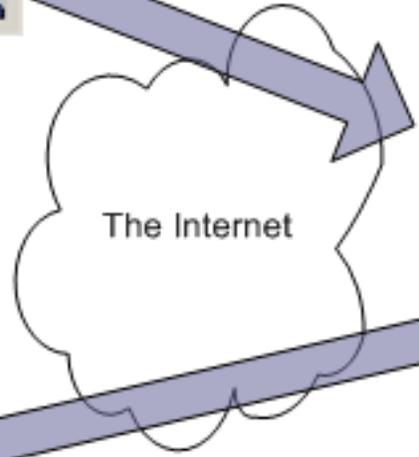
Your Computer

## Document Portfolio

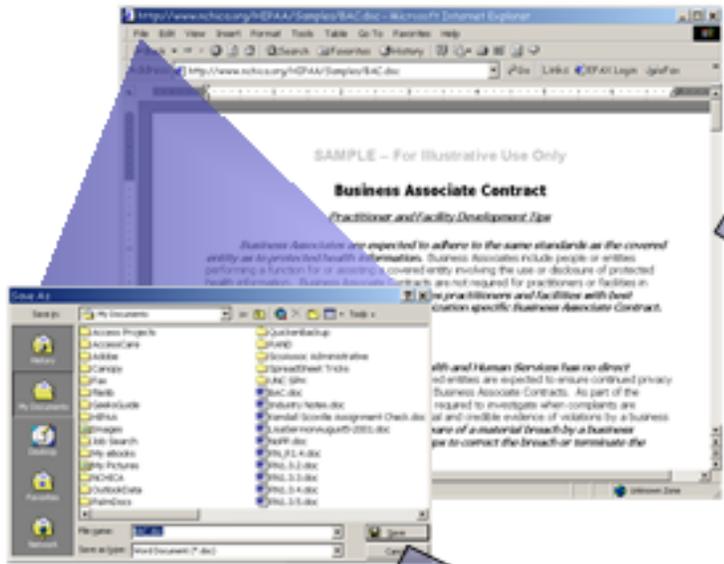


# On-Line Templates

Templates on NCHICA's Web Site



## MS-Word



Save As...

Your Disk

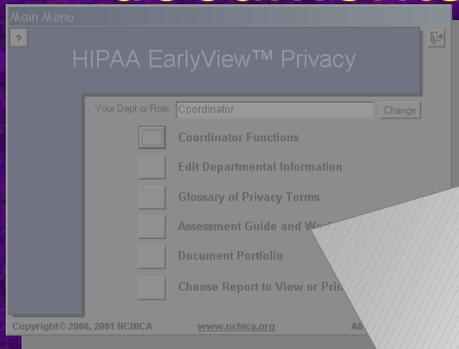


On-line document templates from NCHICA's web site provide a 'jump-start' for preparing your own compliance documents.

# Document Portfolio

A single screen to manage all compliance documents

Local copy available



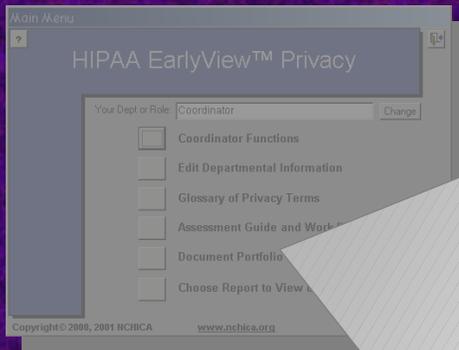
A screenshot of the 'Document Portfolio' application window. The window title is 'Document Portfolio'. The main content area features a table with columns for 'Name of Document', 'Open', 'Required', and 'Available'. The first row is selected, and a callout bubble points to the 'Available' checkbox, which is checked. The footer of the window contains 'Copyright© 2000, 2001 NCHICA', 'www.nchica.org', and 'All Rights Reserved'. At the bottom, a record navigation bar shows 'Record: 1 of 13'.

Name of Document	Open	Required	Available
▶ Authorization Form for the Practice to Release Information	Open	Yes	<input checked="" type="checkbox"/>
Authorization Form for the Practice to Request Information	Open	Yes	<input type="checkbox"/>
Business Associate Contract	Open	Yes	<input type="checkbox"/>
Computer and Information Usage Agreement	Open	No	<input type="checkbox"/>
Consent Form for the Practice	Open	Yes	<input type="checkbox"/>
Notice of Privacy Practices	Open	Yes	<input type="checkbox"/>
Policies and Procedures for Patient PHI Requests	Open	Yes	<input type="checkbox"/>
Policies Regarding "Minimum Necessary" PHI Disclosures	Open	Yes	<input type="checkbox"/>

# Glossary of Terms

A convenient guide to HIPAA terminology

Search for specific terms



A screenshot of the 'Glossary of Privacy Terms' application window. The title bar reads 'Glossary of Privacy Terms'. Below the title bar is a search bar with a question mark icon and a search button. To the right of the search bar are radio buttons for 'Find all' (selected), 'Find any', and 'Exact'. Below the search bar is a table with two columns: 'Term' and 'Definition'. The table lists several terms and their definitions. At the bottom of the window is a footer with 'Copyright© 2000, 2001 NCHICA', 'www.nchica.org', and 'All Rights Reserved'.

Term	Definition
Act (160.103)	[he Social Security Act
ANSI (160.103)	the American National Standards Institute
Authorization (MD Guide)	An authorization is a written document signed by a patient giving permission to a provider to disclose protected health information for purposes other than treatment, payment and health care operations. An
Business Associate (MD Guide)	A person or entity who performs a function for or assists a covered entity or health care arrangement with a function or activity involving the use or disclosure of individually identifiable health information

# Reports

HEVp provides a full range of management reports.

---

## Questions with Any Answer

Report Restricted to Coordinator

Category:

Operational

**Requirement:** Privacy rules require consent for disclosure of PHI for treatment, payment and health care operations, and authorization for all other purposes for which written permission is required. These are different from consents for the treatment of a patient.

- 1 Have you made a distinction between consent and authorization documents and added the appropriate language for use and disclosure of PHI?

Coordinator: No

**Requirement:** Core Elements of an Authorization are: A specific description of the information to be disclosed, the name or other specific identification of the person(s) making the request, expiration date, a statement of the individual's right to revoke, statement that information used or disclosed may be subject to re-disclosure, signature and date, if signed by a representative a description of the authority.

- 3 Does your authorization document contain all the required elements for disclosure of PHI?

Coordinator: No

**Requirement:** A covered entity must limit use or disclosure of PHI to the minimum necessary to carry out the intended purpose of the request.

# Resources

- NCHICA: [www.nchica.org](http://www.nchica.org)
- WEDi/SNIP Web site: [snip.wedi.org](http://snip.wedi.org)
- HIPAA GIVES: [www.hipaagives.org](http://www.hipaagives.org)
- DHHS/HIPAA: [aspe.hhs.gov/admnsimp](http://aspe.hhs.gov/admnsimp)

# NCHICA

North Carolina Healthcare Information &  
Communications Alliance, Inc.

**[www.nchica.org](http://www.nchica.org)**

P.O. Box 13048

Research Triangle Park, NC 27709-3048

Voice: 919.558.9258 or 800.241.4486

Fax: 919.558.2198

[nchica@nchica.org](mailto:nchica@nchica.org)

**Questions ???**