NCHICA’s EarlyView™ Privacy Tool

Canopy Systems, Inc.
1520 E. Franklin St.
Chapel Hill, NC 27514
www.canopysystems.com
800-1-354

March 13-15, 2002
David C. Kibbe, MD  Disclosure

President-

◯ - The AMA Field Guide to HIPAA Implementation

eHealth topics
Adjunct Assistant Professor in Health Policy and Administration at the School of Public Health, University of North Carolina at Chapel Hill
Graduate of Harvard University, Case-

Chairman and Founder of Canopy Systems, Inc.

-based software Canopy®—
community-wide case management, utilization management, and disease management programs at a

Email david kibbe@canopysystems.com
Presentation Topics

• NCHICA and its role in promoting awareness and implementation of HIPAA
  – Mission, non-profit status, accomplishments

• EarlyView™ Security and Privacy Tools
  – Method of development and testing
  – Intended audience and assumptions regarding use

• EarlyView™ Privacy Tool Demo
  – Minimum requirements
  – Software features
  – Flexibility of end-user approaches
  – Ongoing feedback and improvements
Presentation References

• NCHICA Web site
  – www.nchica.org click on
  or
  – Look for “HIPAA information” and “tools”
  – Select “EarlyView Privacy”
  or go directly to:
The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes national standards for ensuring the security and privacy of identifiable patient information. Healthcare providers, health plans and clearinghouses are required to be in full compliance with the new HIPAA standards or face potential civil and criminal penalties.

NCHICA offers powerful self-evaluation software tools to help you assess your organization’s readiness to comply with HIPAA:

- Purchase HIPAA EarlyView™ software tools now
- Learn more about HIPAA EarlyView™ Privacy
- View an on-line presentation and demo of HIPAA EarlyView™ Privacy
- Learn more about HIPAA EarlyView™ Security
- Learn more about the HIPAA regulations
- NCHICA members get the best prices on NCHICA tools. Learn about NCHICA membership
- Affiliates of EarlyView Sponsor Organizations receive special discounts on HIPAA EarlyView™ Find out more
What is NCHICA?

• 501(c)(3) nonprofit research & education

• 200+ members including:
  – Providers
  – Health Plans
  – Clearinghouses
  – Professional Associations and Societies
  – **NCHIMA - Charter Member**
  – Research & Pharmaceutical Organizations
  – Government Agencies - Fed & State
  – Vendors

• **Mission:** Implement information technology and secure communications in healthcare
Some NCHICA Accomplishments

- Over 20 multi-disciplinary focus groups covering HIPAA transactions, privacy, and security
- Publishing of white papers, sample documents, and state pre-emption analyses
- Numerous HIPAA educational activities within North Carolina and nationally
- Involvement in granted research projects
  - PaiRs, a common multi-state immunization registry
  - DeeDs, a standardized public health ER registry
  - HealthKey, a multi-state initiative to research and test public key infrastructure, PKI, in health care
- Development of low cost, high quality tools for compliance with HIPAA security and privacy
NCHICA HIPAA Implementation Planning Task Force

• Goal:
  – Develop overall strategy for addressing HIPAA compliance in an orderly and most efficient manner possible.

• Coordinate Activities of Work Groups:
  – Transactions, Codes & Identifiers
  – Data Security
  – Network Security & Interoperability
  – Privacy
  – Awareness, Education & Training

• Over 300 Participants Involved in Effort
HIPAA At-A-Glance

HIPAA Administrative Simplification

Transaction Standards

Data Sets
- ASC x12N version mandated; NCPDP required for pharmacy transactions
  - Eligibility 270/271
  - Benefit enrollment 834
  - Referral cert. and authorization 278
  - Claims 837
  - Claim status 276/277
  - Claim paymt & remittance advice 835
  - Premium payment 820
  - Add’tnl info to support claim 275 (not yet final)
  - First report of injury 148

Code Sets
- ICD-9-CM
- CPT-4
- HCPCS
- CDT
- NDC (and possibly J codes)
- No local codes permitted

Standard Codes

Privacy

New Rights
- Pts access to and control over protected health info (PHI)
- Pts must authorize use of PHI for research or marketing

New Obligations
- PHI data defined
- Notice of privacy practices
- Consent for routine use of PHI
- Minimum disclosure or use
- Business associate contracts
- Provider designated Privacy Official

Security

Administrative Procedures
- Security officer
- Contingency and disaster recovery
- Training

Phys Safeguards
- Secure workstations
- Physical access controls
- Training

Technical Security
- Access controls
- Authorization
- Data authentication
- Encryption, firewalls, etc.
- Basic network security

Unique Identifiers

Provider
- Single NPI: 10-position numeric, 1-digit checksum
- No embedded intelligence

Employer
- 9-position numeric, digit checksum
- Tax ID number
- No imbedded intelligence

Health Plan
- 10+3 position numeric
- Sub-ID may appear on health card

Individual
- Not likely to be finalized
## HIPAA At-A-Glance

<table>
<thead>
<tr>
<th>Standard Set Name</th>
<th>Date of Final Rule Publication</th>
<th>Deadline for Implementation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Standards</strong></td>
<td>Published by HHS December 28, 2000, but effective date is April 14, 2001</td>
<td>April 14, 2003</td>
<td>A Guidance was issued by HHS in July, 2001, and a further Final Rule with clarifications is expected in 2002, second quarter.</td>
</tr>
<tr>
<td><strong>Security Standards</strong></td>
<td>HHS has published a proposed rule (NPRM) in May, 1998.</td>
<td>None yet. April 14, 2003 for security provisions included in Privacy Rule.</td>
<td>The Security Final Rule is expected in first or second quarter 2002, and is not expected to change substantially from the proposed form of the rule.</td>
</tr>
<tr>
<td><strong>National Identifier Standards</strong></td>
<td>HHS has published a proposed rule (NPRM, 1998) for a National Provider Identifier, and a National Employer Identifier</td>
<td>None yet.</td>
<td>National Health Plan Identifier is under development, and a National Individual Identifier is on hold.</td>
</tr>
</tbody>
</table>

*CANOPY SYSTEMS, INC.*
HIPAA Privacy Overview

HIPAA Administrative Simplification

Consents and Authorizations

Consents
- Required for PHI use for treatment, payment, or healthcare operations
- Pt may request restriction
- Joint consent allowed
- Requires process

Authorizations
- Authorization separate, required for all other disclosures of PHI not covered by consent (e.g., research, marketing, psychotherapy notes)
- May be revoked

Uses and Disclosures

- Duty not to disclose PHI except as permitted
- Required to disclose to the individual
- Un-identification defined
- Business associate contracts required
- Personal reps allowed to view PHI
- Notice of Privacy Practices posted
- Whistleblowers allowed
- Targeted marketing allowed without auth (may change)
- Use of PHI for fundraising permitted
- Uses required by law, public health, oversight, decedents, research, etc.
- Minimum necessary and "need to know" req.

Consumer Controls

Notification
- Details of document
- Frequency, timing, etc.

Communications
- Patients have right to request access to PHI
- May be denied under some circumstances
- Patients have right to amend PHI w/ exceptions
- Fees limited to costs

Process
- Patient has right to accounting of disclosure for 6 yrs prior to request with exceptions
- Procedures required!

Administration and Security

Administration
- Privacy Official required
- Training on privacy
- Complaints
- Employee sanctions
- Policies and procedures implemented and specific to org. size

Security
- Admin, physical, and technical safeguards to protect PHI
- Implementation guide reasonable, appropriate
- Security regs will give details (expected late 2001)
Definition - Privacy

- **Privacy** is the patient's right over the use and disclosure of his or her own personal health information. Privacy includes the right to determine when, how and to what extent personal information is shared with others. The HIPAA privacy rules grant new rights to patients to gain access to and control the use and disclosure of their personal health information.
Definition - PHI

• Protected health information (PHI) is the HIPAA term for health information in any form (i.e., paper, electronic or verbal) that personally identifies a patient. This includes individually identifiable health information in paper records that have never been electronically stored or transmitted. It does not include data that have been "dis-identified" by removal of identifying information, such as name, address, ZIP code, etc.
New Patient Rights

- To control the use and disclosure of protected health information
- To request to review and amend personal health information
- To revoke consent or authorization for use of personal health information

- Applies to all forms of health information, including paper
- There are exceptions and qualifications
New Provider Obligations

- To have and use a Notice of Privacy Practices
- To obtain consents and authorizations for use of PHI
- To abide by “minimum necessary” guidelines
- To assure business associates comply with HIPAA
- To put in place adequate security measures, including administrative, physical safeguards, and technical security measures to protect PHI
- To train employees
- To appoint a privacy official
Steps to Compliance

• Begin Awareness
• Form HIPAA Team
• Initiate Gap Analysis
• Perform Risk Analysis
• Develop Your Compliance Plan, Budget & Timeline
• Execute Plan
• Revaluate and Adjust Plan
Comes close to being
“HIPAA Privacy Compliance In a Box”
For Medical Practice

www.nchica.org/e-commerce/evinf.htm
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 compliance documents
Downloadable from NCHICA web site

Microsoft Access™
Database application
Runs on Windows 95/98/2000
## Minimum Requirements

<table>
<thead>
<tr>
<th></th>
<th>Access 2000</th>
<th>Access ’97</th>
<th>RunTime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disk Space</strong></td>
<td>3.5 MB</td>
<td>3.0 MB</td>
<td>43 MB</td>
</tr>
<tr>
<td><strong>MS-Access</strong></td>
<td>2000, 2002, XP</td>
<td>’97</td>
<td>None</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>Pentium II, 32 MB memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internet</strong></td>
<td>High speed internet connection recommended</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MS-Word</strong></td>
<td>2000, 2002, XP</td>
<td>’97</td>
<td>‘95</td>
</tr>
</tbody>
</table>
Tour of

HIPAA EarlyView™

Privacy
Login

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

The Coordinator password is initially blank.
Main Menu

Provides access to all HEV features

Help is available for most functions.
Assessment Guide and Work Plan

For each requirement: clarification, assessment, action items
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.
Rule Text

Shows actual text of the Privacy rule for each requirement

Rule text linked from NCHICA’s web site
Best Practices Advice

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

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.
Work Plan

Each requirement has a set of action items for compliance.

Expanded description of suggested action

Documents required for compliance
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 on-line template

Link to local document
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
Glossary of Terms
A convenient guide to HIPAA terminology

Search for specific terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act [160.103]</td>
<td>[the Social Security Act]</td>
</tr>
<tr>
<td>ANSI [160.103]</td>
<td>the American National Standards Institute</td>
</tr>
<tr>
<td>Authorization (MD Guide)</td>
<td>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.</td>
</tr>
<tr>
<td>Business Associate (MD Guide)</td>
<td>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</td>
</tr>
</tbody>
</table>
Reports

HEVp provides a full range of management reports.

Questions with Any Answer

Report Restricted to Coordinator

<table>
<thead>
<tr>
<th>Category:</th>
<th>Operational</th>
</tr>
</thead>
</table>

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.
Caveats

• To keep cost to a minimum, HEVp is distributed “as is,” without technical or other support.

• Documents and templates are for example only. HEVp does not provide all documents that will be required by the regulations or by state laws.

• Users should consult their legal counsel prior to adoption of any document.

• NCHICA cannot and will not accept any legal liability arising from the use of these tools or associated documents.
Resources

• NCHICA: www.nchica.org

• WEDi/SNIP Web site: snip.wedi.org

• DHHS/HIPAA: aspe.hhs.gov/admnsimp
On the Internet,
Nobody Knows You're a Dog

"On the Internet, nobody knows you're a dog."