One Year to Go - Getting Started with Your HIPAA Security Self-Assessment and Planning

Presented to:

HIPAA Summit VIII
Baltimore, Maryland
March 8, 2004

Holt Anderson, Executive Director

North Carolina Healthcare Information & Communications Alliance, Inc.

Presentation Segments

- Introduction to Gap and Risk Analysis:
  - Regulation overview
  - Compliance
  - Beginning the Process
  - Gap analysis
  - Risk assessment
  - Maintaining Compliance
- Q&A

Security Regulation Overview

§ 164.306 Security standards: General rules

(a) General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

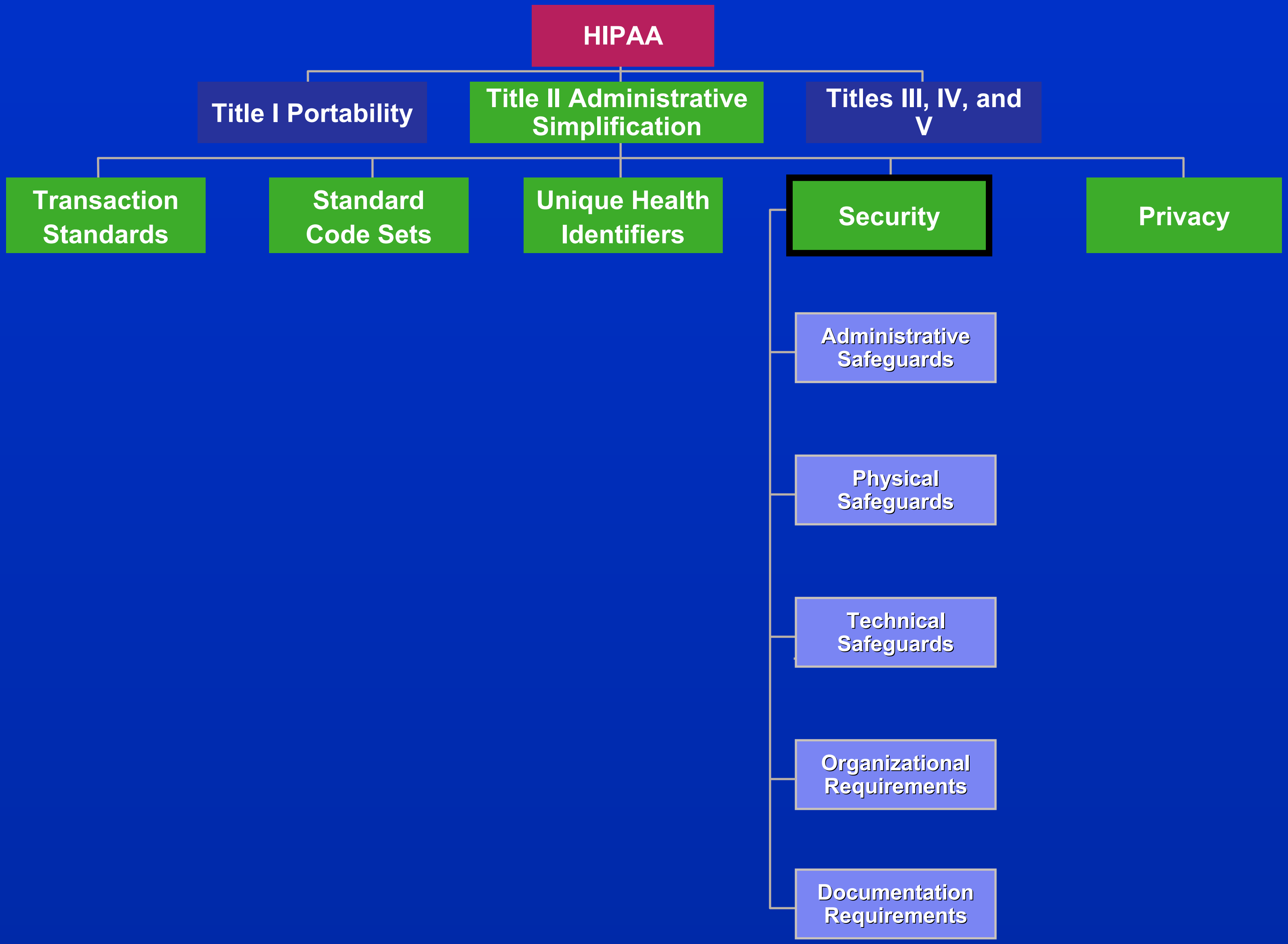
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

NCHICA

§ 164.306 Security standards: General rules

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.



HIPAA

Title I Portability

Title II Administrative Simplification

Titles III, IV, and V

Transaction Standards

Standard Code Sets

Unique Health Identifiers

Security

Privacy

Administrative Safeguards

Physical Safeguards

Technical Safeguards

Organizational Requirements

Documentation Requirements

ERNST & YOUNG

FROM THOUGHT TO FINISH.™

Security Regulation

- Administrative Safeguards
  - 12 Required Specifications
  - 11 Addressable Specification
- Physical Safeguards
  - 4 Required, 6 Addressable
- Technical Safeguards
  - 4 Required, 5 Addressable
- Organizational Requirements
  - 6 Required, 0 Addressable
- Policies & Procedures Documentation Requirements
  - 6 Required, 0 Addressable

Specifications

- Required
  - Must be implemented
- Addressable
  - Implement one or more specifications
  - Implement one or more alternative measures
  - Implement a combination of both
  - Not implement specification
  - BUT, rationale must be documented

Compliance & Enforcement

Business Risks

- Loose security implementation may open the door to litigation for privacy violations
- Not adjusting as scope and complexity of current environment / technology changes
- Unquestioning reliance on vendors and “HIPAA Compliant” solutions
- Not completing a thorough analysis / compliance effort and is found negligent

Impact of Not Complying

- Possible litigation
- Loss of public confidence
- Penalties
  - Civil monetary for violations of each standard
  - Criminal for wrongful disclosure of protected health information
  - No private right of action

Medical Security Case

Alleged Holly Springs Hacker Wanted To Show Flaws In Security

Clayton Dillard Accused Of Unlawfully Accessing Hospital Computer System

POSTED: 11:06 a.m. EDT September 9, 2003

RALEIGH, N.C. -- A Holly Springs man is in trouble after being accused of hacking into a medical office's wireless computer network.

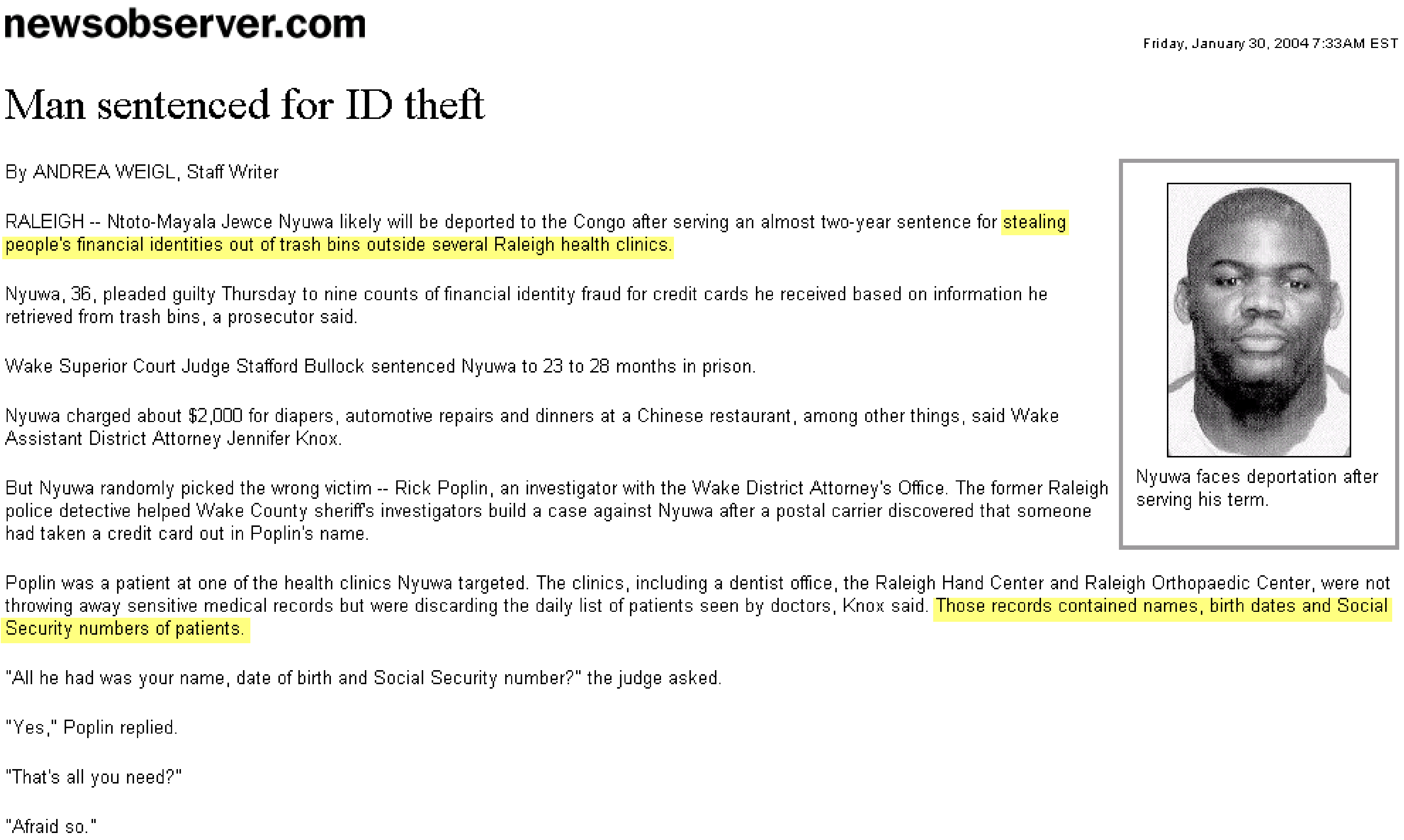
Clayton Dillard is accused of hacking into a hospital computer system and accessing information of hundreds of patients.

Raleigh police said Clayton Taylor Dillard, a 29-year-old information security consultant, is charged with one felony count of computer trespass, one felony count of unlawful computer access and one misdemeanor count of computer trespass. They said the charges against Dillard resulted from an intrusion that occurred to a wireless computer network at Wake Internal Medicine Consultants Inc. After Dillard accessed the information, he contacted patients and insurance companies. He also wrote WRAL a letter, stating, "These guys are a bunch of bozos." He also mailed WRAL copies of checks and insurance forms with patient names and procedures.

http://www.wral.com/news

NCHICA

Medical Security Case



newsobserver.com

Friday, January 30, 2004 7:33AM EST

Man sentenced for ID theft

By ANDREA WEIGL, Staff Writer

RALEIGH -- Ntoto-Mayala Jewce Nyuwa likely will be deported to the Congo after serving an almost two-year sentence for stealing people's financial identities out of trash bins outside several Raleigh health clinics.

Nyuwa, 36, pleaded guilty Thursday to nine counts of financial identity fraud for credit cards he received based on information he retrieved from trash bins, a prosecutor said.

Wake Superior Court Judge Stafford Bullock sentenced Nyuwa to 23 to 28 months in prison.

Nyuwa charged about $2,000 for diapers, automotive repairs and dinners at a Chinese restaurant, among other things, said Wake Assistant District Attorney Jennifer Knox.

But Nyuwa randomly picked the wrong victim -- Rick Poplin, an investigator with the Wake District Attorney's Office. The former Raleigh police detective helped Wake County sheriff's investigators build a case against Nyuwa after a postal carrier discovered that someone had taken a credit card out in Poplin's name.

Nyuwa faces deportation after serving his term.

Poplin was a patient at one of the health clinics Nyuwa targeted. The clinics, including a dentist office, the Raleigh Hand Center and Raleigh Orthopaedic Center, were not throwing away sensitive medical records but were discarding the daily list of patients seen by doctors, Knox said. Those records contained names, birth dates and Social Security numbers of patients.

"All he had was your name, date of birth and Social Security number?" the judge asked.

"Yes," Poplin replied.

"That's all you need?"

"Afraid so."

HIPAA Enforcement

- **Office of Civil Rights (Privacy)**
- **CMS (Transactions, Code Sets, Identifiers, Security)**
- Justice Department
- FBI
- OIG (Re: lessons learned from fraud & abuse)
- Accreditation reviews
- Plaintiff's bar & courts
- Business Continuity

HIPAA Enforcement at CMS

New office established in CMS:

- » Establish and operate enforcement processes
- » Develop regulations
- » Obtaining voluntary compliance through technical assistance
- » Process will be complaint driven

Beginning the Process

Beginning the Process

For a large organization:

- Determine scope of project (incl. other regulations)
- Obtain top management approval
- Engage key players from each affected area
- Build assessment team
- Train assessment team to “standard” of assessment
- Do the assessments
- Craft a Compliance Plan

Beginning the Process

For a small organization (practice):

- Determine scope of project
- Bring in outside trusted advisor / consultant
- Do the assessment(s)
- Craft a Compliance Plan
- Select vendors
- Work toward compliance

Gap Analysis

Gap Analysis

- What is your current state?
- What do the regulations say?
  - Required Standards
  - Addressable Standards
- Where is the mismatch (gap)?
- What is ***reasonable and appropriate*** to do within a tolerable risk?

Planning for Your Gap Analysis

- Utilize information already in hand:
  - Inventories of hardware and applications
  - Existing policies and procedures
- Methodically review each of the Security Standards and Specifications to determine their applicability to your organization.
- Consider HIPAA's interaction with other laws, regulations and standards that apply to you.

During & After Information Gathering

- Document Findings
  - **Key areas of concern**
  - **Trends**
- Construct alternative paths to compliance
  - **Business impacts / risks**
  - **Clinical impacts of alternatives**
- Formalize risk assessment
- Make choices and proceed with an implementation plan leading to compliance

Security Management Process

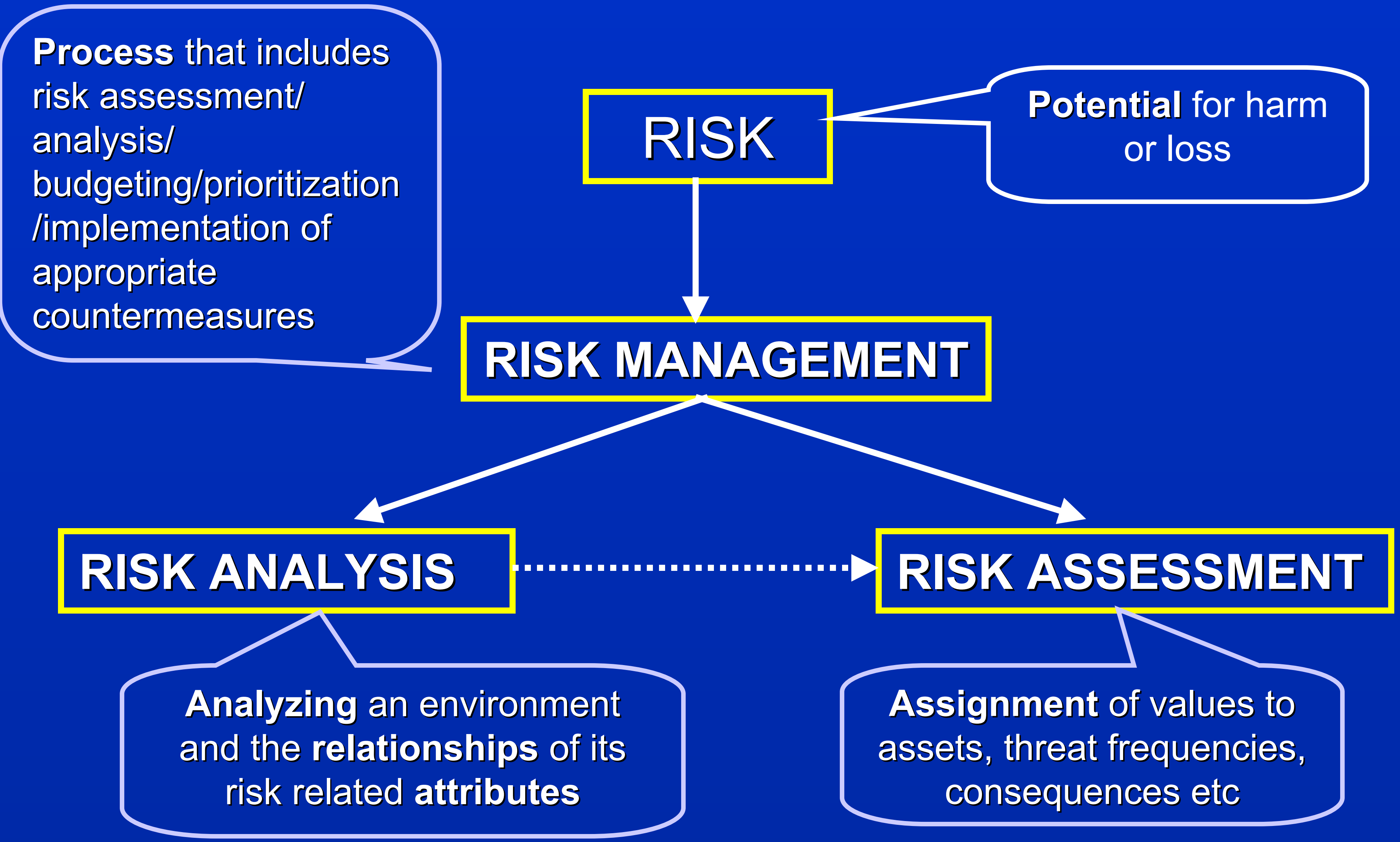
- Process to prevent, detect, contain, and correct threats, vulnerabilities and exposures
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review

Risk Assessment

Risk Assessment

- § 164.308 Administrative Safeguards
  - Implementation specifications
    - (A) **Risk Analysis** (Required) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information by the covered entity.
    - (B) **Risk Management** (Required) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)

Definitions



RISK

Potential for harm or loss

RISK MANAGEMENT

Process that includes risk assessment/ analysis/ budgeting/prioritization /implementation of appropriate countermeasures

RISK ANALYSIS

RISK ASSESSMENT

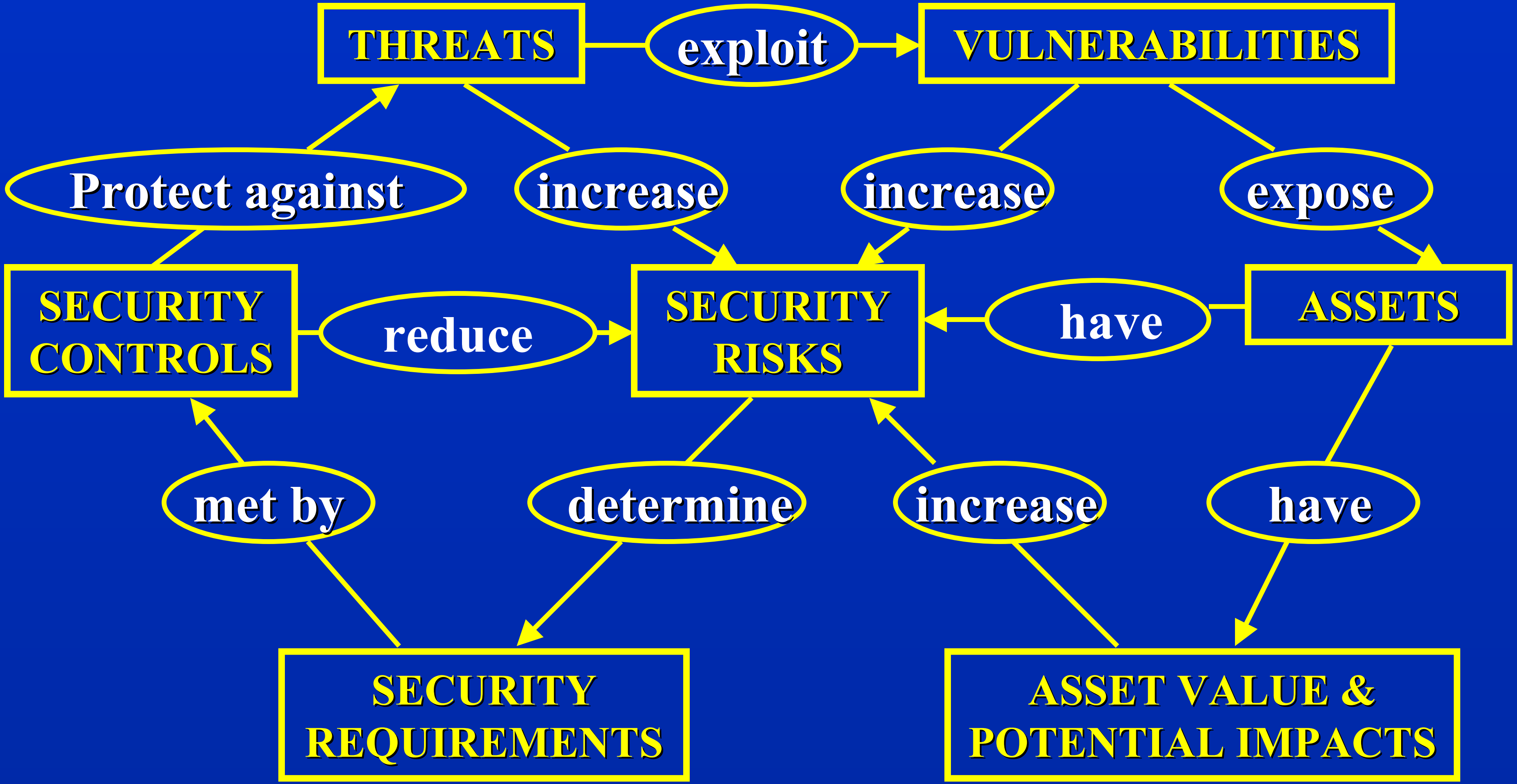
Analyzing an environment and the **relationships** of its risk related **attributes**

Assignment of values to assets, threat frequencies, consequences etc

UAB THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

NCHICA

Risk Components Relationship



Benefits of Risk Assessment

- Some of the specific benefits include:
  - Understand *what is at risk*
  - The *value at risk* – i.e. information assets and with confidentiality, integrity and availability of assets
  - *Kinds of threats* and their financial consequences
  - *Mitigation analysis*: what can be done to reduce risk to an acceptable level

Two types of Risk Assessment

- **Quantitative** – dollar values / metrics / real numbers
  - More complex / accurate / tedious
  - Cost benefit analysis provided
  - Independent objective methods
  - clear
- **Qualitative** – ranking - high med low
  - Allows for owners / users / expert input as to value
  - Faster / easier
  - Less accurate

Security Management Process

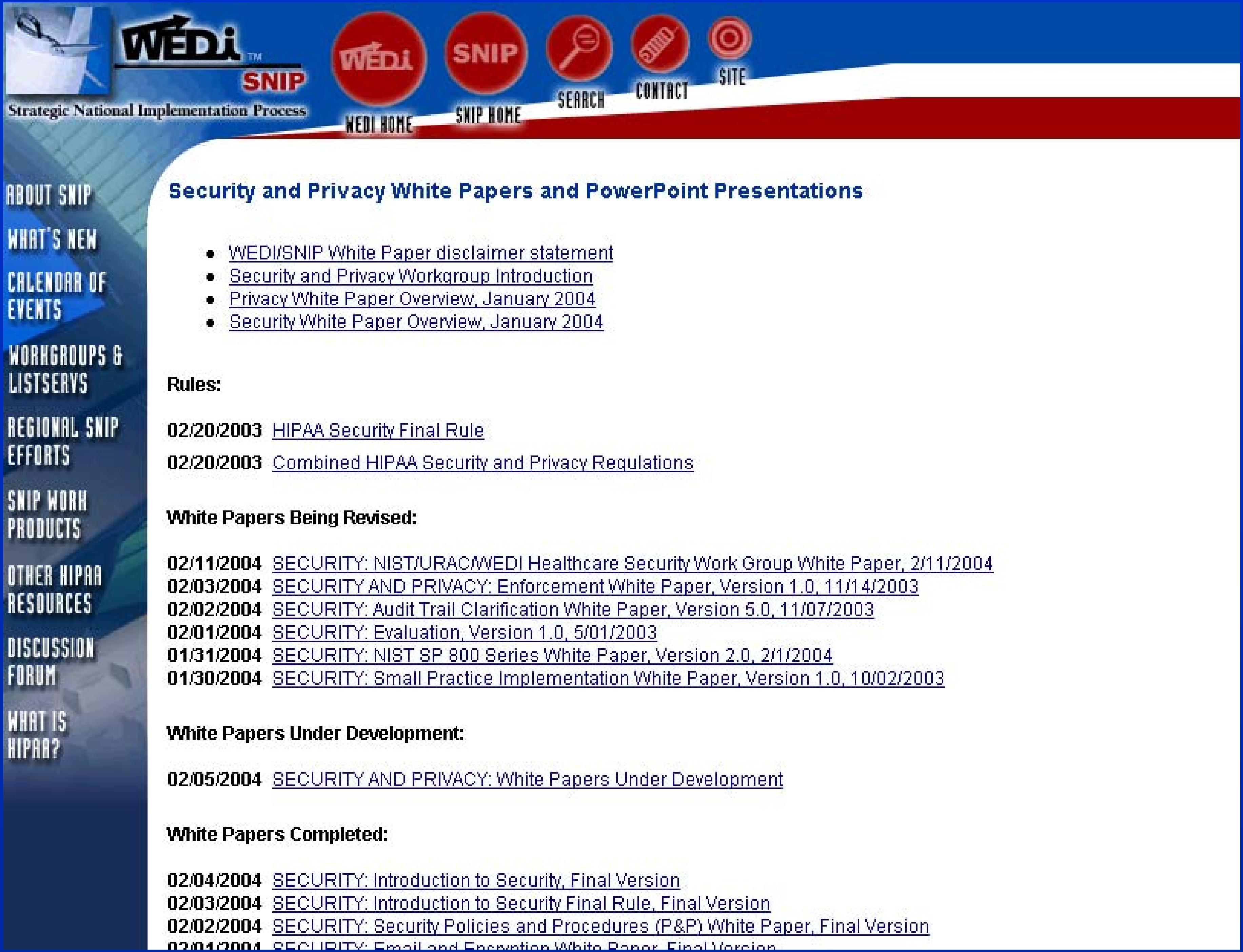
- Process to prevent, detect, contain, and correct threats, vulnerabilities and exposures
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review

Now that you are through…

Updating and Maintaining Compliance

- Consider updates after implementing:
  - New processes
  - Changes in:
    - Workflows
    - Responsibilities
    - Laws
    - Standards/practices
    - Technology – hard and soft
  - Every 3 years as a minimum under HIPAA
    - Constant process for most

Examples of Tools and Other Resources That Can Facilitate Your Gap Analysis and Risk Assessment



Security and Privacy White Papers and PowerPoint Presentations

- WEDI/SNIP White Paper disclaimer statement
- Security and Privacy Workgroup Introduction
- Privacy White Paper Overview, January 2004
- Security White Paper Overview, January 2004

Rules:

02/20/2003 HIPAA Security Final Rule

02/20/2003 Combined HIPAA Security and Privacy Regulations

White Papers Being Revised:

02/11/2004 SECURITY: NIST/URAC/WEDI Healthcare Security Work Group White Paper, 2/11/2004
02/03/2004 SECURITY AND PRIVACY: Enforcement White Paper, Version 1.0, 11/14/2003
02/02/2004 SECURITY: Audit Trail Clarification White Paper, Version 5.0, 11/07/2003
02/01/2004 SECURITY: Evaluation, Version 1.0, 5/01/2003
01/31/2004 SECURITY: NIST SP 800 Series White Paper, Version 2.0, 2/1/2004
01/30/2004 SECURITY: Small Practice Implementation White Paper, Version 1.0, 10/02/2003

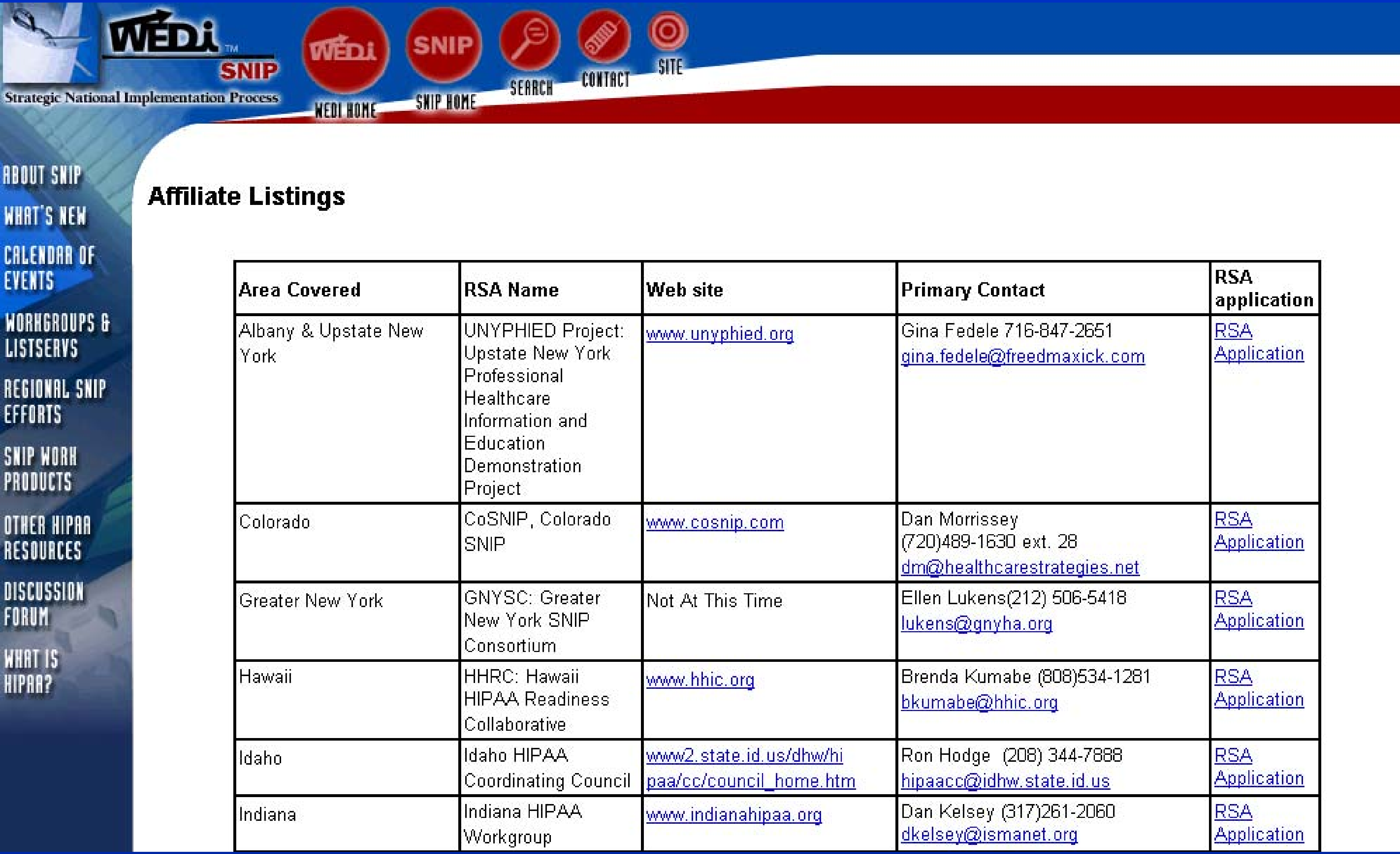
White Papers Under Development:

02/05/2004 SECURITY AND PRIVACY: White Papers Under Development

White Papers Completed:

02/04/2004 SECURITY: Introduction to Security, Final Version
02/03/2004 SECURITY: Introduction to Security Final Rule, Final Version
02/02/2004 SECURITY: Security Policies and Procedures (P&P) White Paper, Final Version
02/01/2004 SECURITY: Email and Encryption White Paper, Final Version

Help in your own community ?



Affiliate Listings

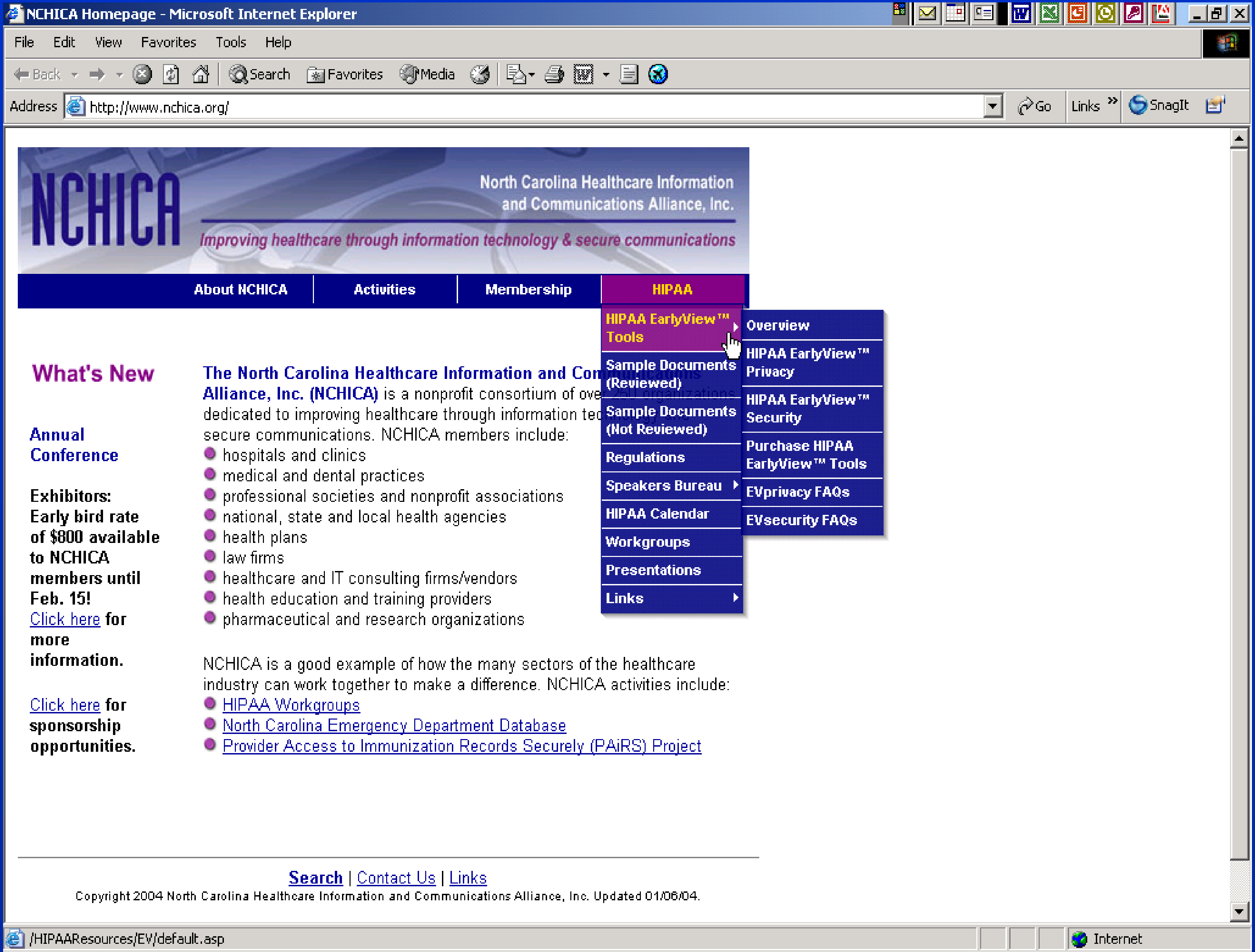
Area Covered	RSA Name	Web site	Primary Contact	RSA application
Albany & Upstate New York	UNYPHIED Project: Upstate New York Professional Healthcare Information and Education Demonstration Project	www.unyphied.org	Gina Fedele 716-847-2651 gina.fedele@freedmaxick.com	RSA Application
Colorado	CoSNIP, Colorado SNIP	www.cosnip.com	Dan Morrissey (720)489-1630 ext. 28 dm@healthcarestrategies.net	RSA Application
Greater New York	GNYSC: Greater New York SNIP Consortium	Not At This Time	Ellen Lukens(212) 506-5418 lukens@gnyha.org	RSA Application
Hawaii	HHRC: Hawaii HIPAA Readiness Collaborative	www.hhic.org	Brenda Kumabe (808)534-1281 bkumabe@hhic.org	RSA Application
Idaho	Idaho HIPAA Coordinating Council	www2.state.id.us/dhw/hipaa/cc/council_home.htm	Ron Hodge (208) 344-7888 hipaacc@idhw.state.id.us	RSA Application
Indiana	Indiana HIPAA Workgroup	www.indianahipaa.org	Dan Kelsey (317)261-2060 dkelsey@ismanet.org	RSA Application

About NCHICA

- 501(c)(3) nonprofit research & education
- Established in 1994
- ~250 organization members including:
  - **Providers**
  - **Health Plans**
  - **Clearinghouses**
  - **State & Federal Government Agencies**
  - **Professional Associations and Societies**
  - **Research Organizations**
  - **Vendors**
- Mission: Improve healthcare in NC by accelerating the adoption of information technology

NCHICA's HIPAA Efforts

- Task Force and 5 Work Groups
  - **450+ individuals participating from members**
  - **Leverage efforts among organizations**
  - **Build consensus and best practices**
  - **Developed documents, training, and tools**
- Gap analysis tools designed to provide an early cut at self-assessment
- Education has been pleasant by-product
- Consultants use tools to provide consistency and thoroughness in approach for smaller organizations


NCHICA Homepage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.nchica.org/
Go Links SnagIt
NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.
Improving healthcare through information technology & secure communications
About NCHICA
Activities
Membership
HIPAA
HIPAA EarlyView™ Tools
Sample Documents (Reviewed)
Sample Documents (Not Reviewed)
Regulations
Speakers Bureau
HIPAA Calendar
Workgroups
Presentations
Links
Overview
HIPAA EarlyView™ Privacy
HIPAA EarlyView™ Security
Purchase HIPAA EarlyView™ Tools
EVprivacy FAQs
EVsecurity FAQs
/HIPAAResources/EV/default.asp
Internet

What's New

Annual Conference

Exhibitors: Early bird rate of $800 available to NCHICA members until Feb. 15! Click here **for more information.**

Click here **for sponsorship opportunities.**

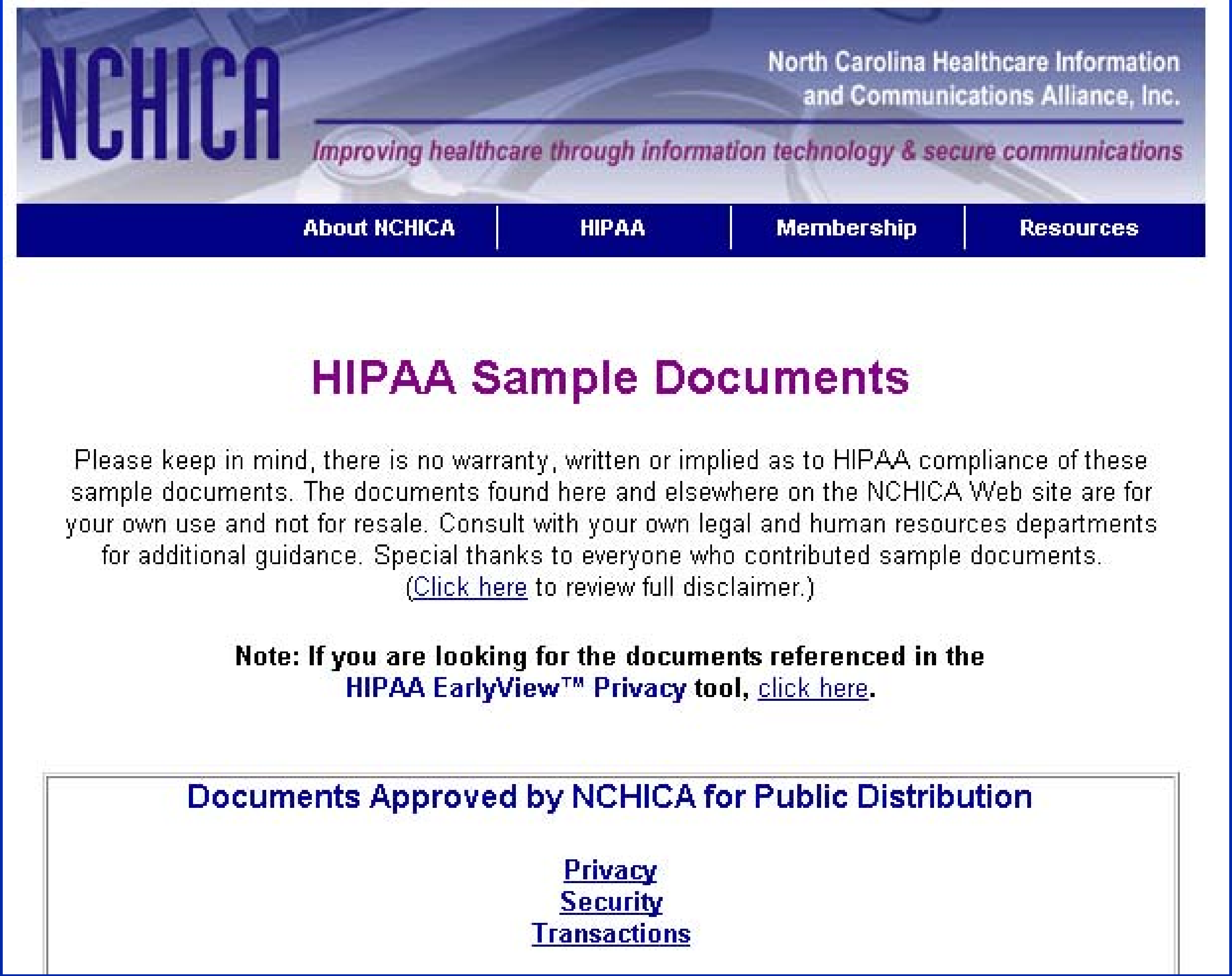
The North Carolina Healthcare Information and Com Alliance, Inc. (NCHICA) is a nonprofit consortium of ove dedicated to improving healthcare through information tec secure communications. NCHICA members include:

- hospitals and clinics
- medical and dental practices
- professional societies and nonprofit associations
- national, state and local health agencies
- health plans
- law firms
- healthcare and IT consulting firms/vendors
- health education and training providers
- pharmaceutical and research organizations

NCHICA is a good example of how the many sectors of the healthcare industry can work together to make a difference. NCHICA activities include:

- HIPAA Workgroups
- North Carolina Emergency Department Database
- Provider Access to Immunization Records Securely (PAiRS) Project

Search | Contact Us | Links



North Carolina Healthcare Information
and Communications Alliance, Inc.

Improving healthcare through information technology & secure communications

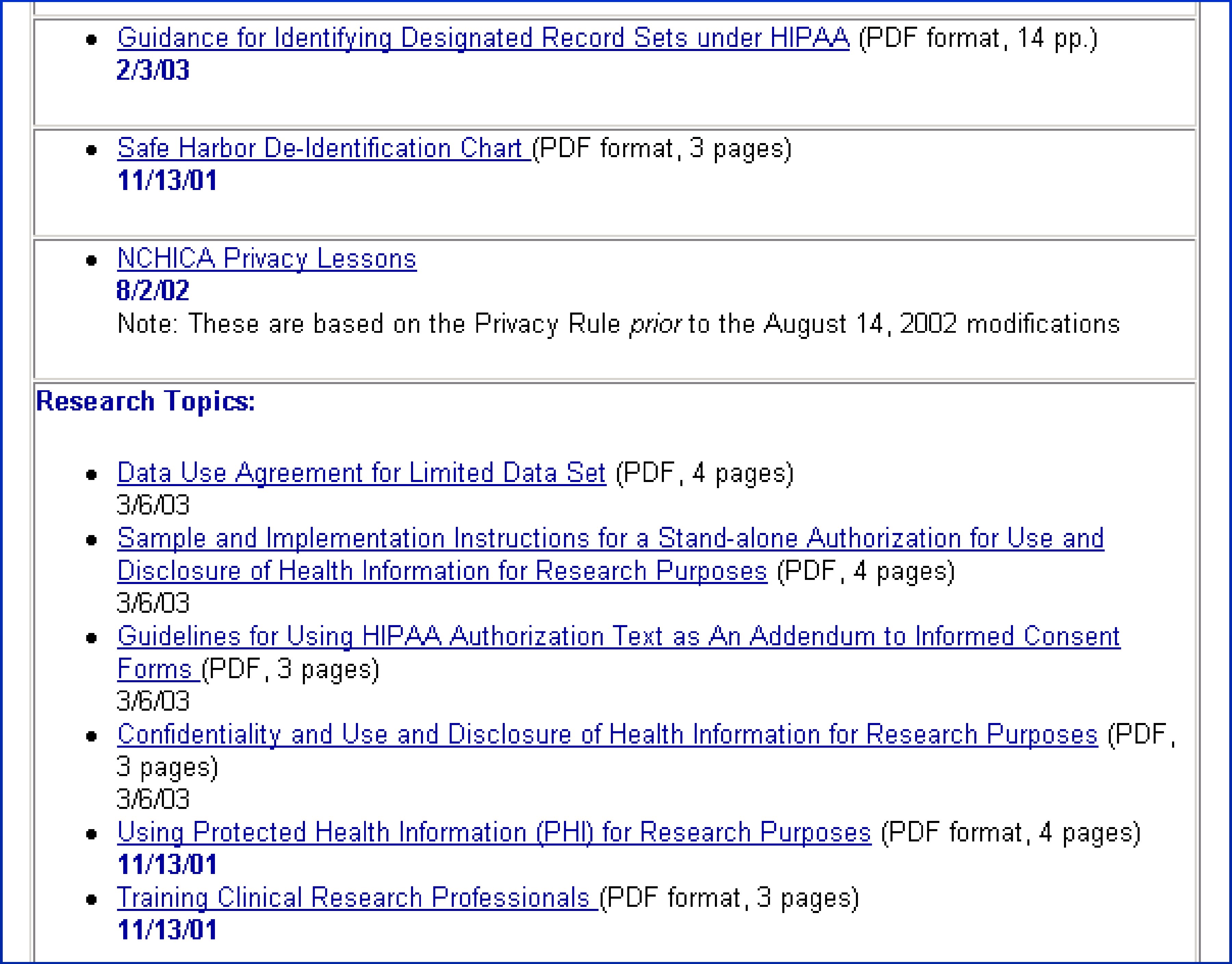
HIPAA Sample Documents

Please keep in mind, there is no warranty, written or implied as to HIPAA compliance of these sample documents. The documents found here and elsewhere on the NCHICA Web site are for your own use and not for resale. Consult with your own legal and human resources departments for additional guidance. Special thanks to everyone who contributed sample documents.
(Click here to review full disclaimer.)

Note: If you are looking for the documents referenced in the
HIPAA EarlyView™ Privacy tool, click here**.**

Documents Approved by NCHICA for Public Distribution

Privacy
Security
Transactions



- Guidance for Identifying Designated Record Sets under HIPAA (PDF format, 14 pp.)
  2/3/03

- Safe Harbor De-Identification Chart (PDF format, 3 pages)
  11/13/01

- NCHICA Privacy Lessons
  8/2/02
  Note: These are based on the Privacy Rule *prior* to the August 14, 2002 modifications

Research Topics:

- Data Use Agreement for Limited Data Set (PDF, 4 pages)
  3/6/03
- Sample and Implementation Instructions for a Stand-alone Authorization for Use and Disclosure of Health Information for Research Purposes (PDF, 4 pages)
  3/6/03
- Guidelines for Using HIPAA Authorization Text as An Addendum to Informed Consent Forms (PDF, 3 pages)
  3/6/03
- Confidentiality and Use and Disclosure of Health Information for Research Purposes (PDF, 3 pages)
  3/6/03
- Using Protected Health Information (PHI) for Research Purposes (PDF format, 4 pages)
  11/13/01
- Training Clinical Research Professionals (PDF format, 3 pages)
  11/13/01

Self-assessment / Gap Analysis Tools

HIPAA EarlyView™ Security

Focus on your compliance plan with this powerful software tool

HIPAA EarlyView™ Privacy

Focus on your compliance plan with this powerful software tool

Goals of EarlyView™ Tools

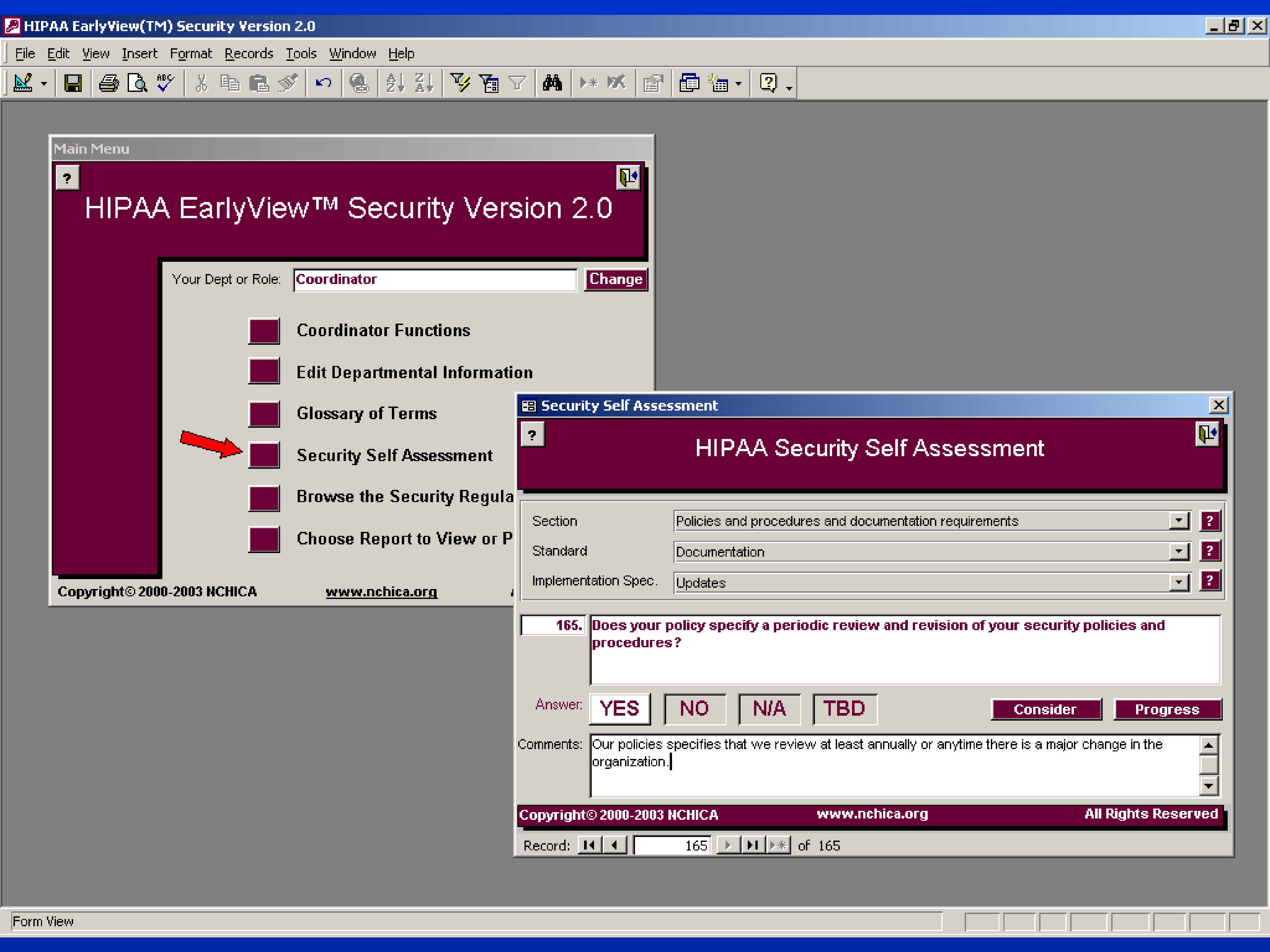
- Develop a clear understanding of the rule and the impact on the organization
  - Management reports highlight action items and document due diligence
- Closed-end gap questions true to the regulation
  - No "extra" questions
  - No room for "Maybe" – only "Yes" "No" or "N/A"
- "Things to think about" provided to expand considerations of how one might approach a particular standard
  - Potential alternatives to compliance

NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc

The Tool's Structure

- Built around the assessment process
- Every requirement / specification covered
- Questions keyed to the regulation standards
- Space for free-text documentation of due diligence
- Presented in same order as regulation
- Links to the regulation text
- Documentation of progress available for management purposes
- Can be updated and new management reports printed as compliance progresses

NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.



HIPAA EarlyView™ Security Version 2.0

Your Dept or Role: Coordinator

Copyright© 2000-2003 NCHICA www.nchica.org

HIPAA Security Self Assessment

Section: Policies and procedures and documentation requirements

Standard: Documentation

Implementation Spec.: Updates

165. **Does your policy specify a periodic review and revision of your security policies and procedures?**

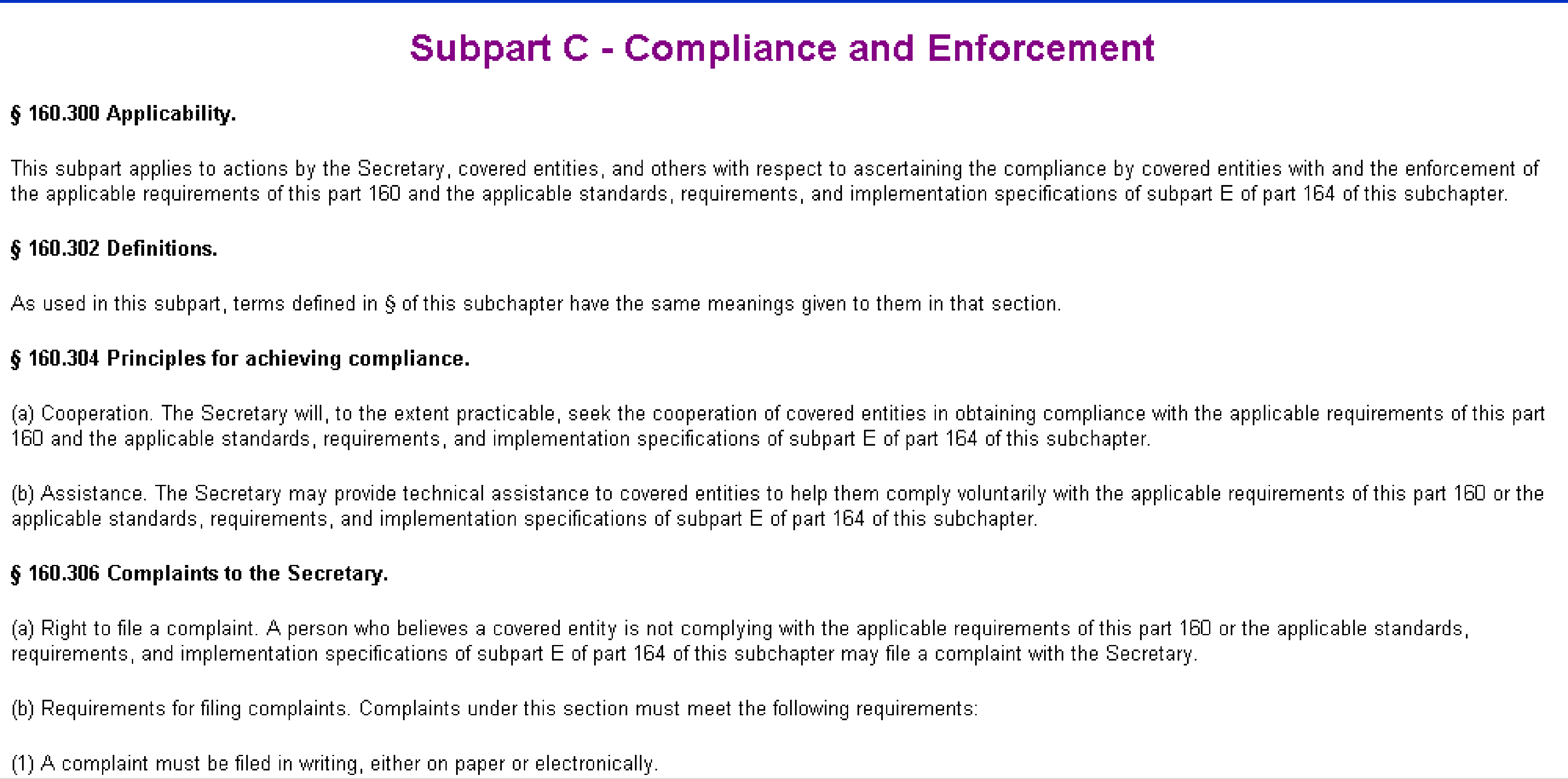
Answer: YES NO N/A TBD

Comments: Our policies specifies that we review at least annually or anytime there is a major change in the organization.

Copyright© 2000-2003 NCHICA www.nchica.org All Rights Reserved

Record: 165 of 165

Links to the Regulation Text



Subpart C - Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) Cooperation. The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) Assistance. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

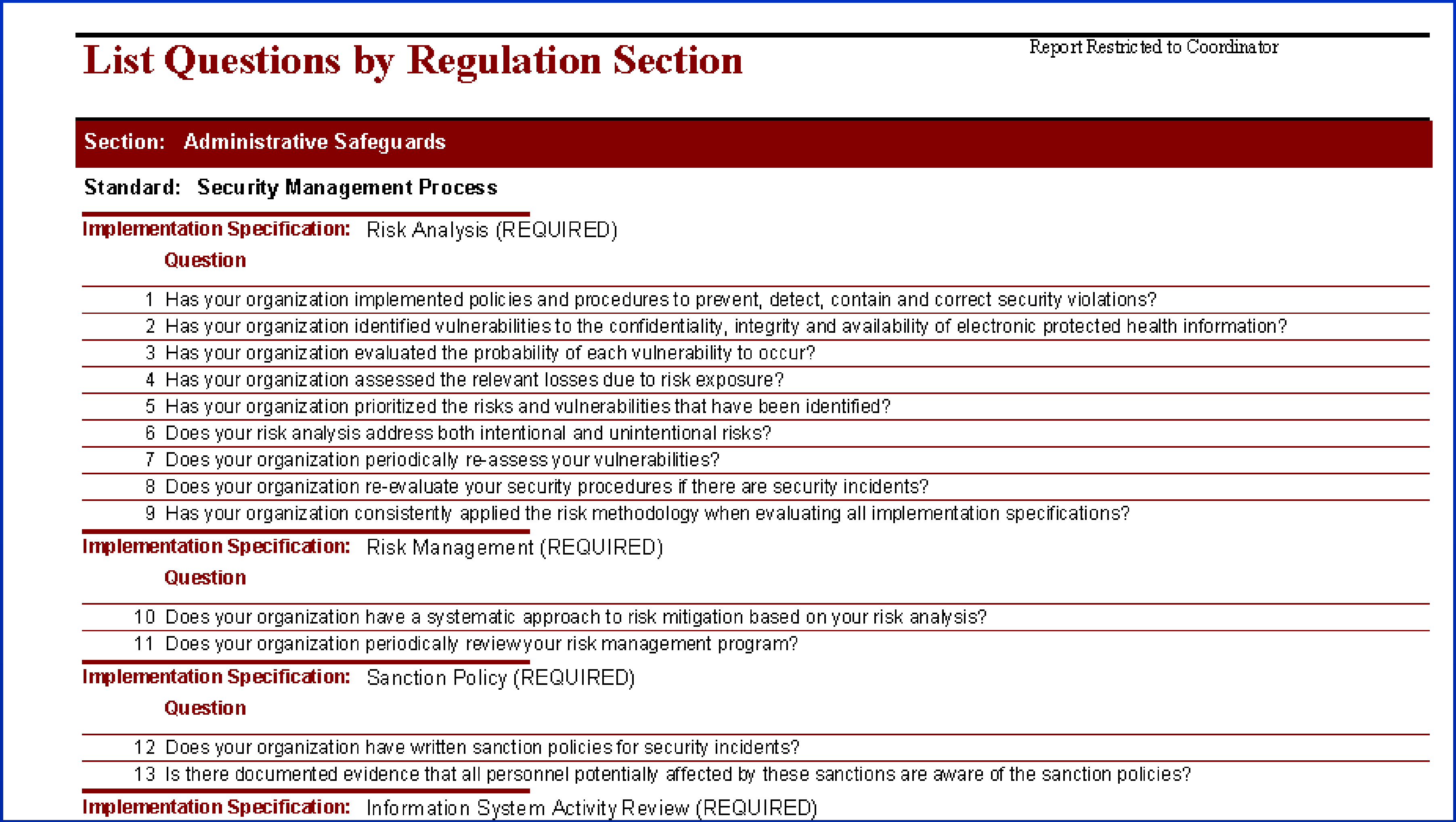
§ 160.306 Complaints to the Secretary.

(a) Right to file a complaint. A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) Requirements for filing complaints. Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

Management Reports



List Questions by Regulation Section

Report Restricted to Coordinator

Section: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: Risk Analysis (REQUIRED)

Question

1 Has your organization implemented policies and procedures to prevent, detect, contain and correct security violations?

2 Has your organization identified vulnerabilities to the confidentiality, integrity and availability of electronic protected health information?

3 Has your organization evaluated the probability of each vulnerability to occur?

4 Has your organization assessed the relevant losses due to risk exposure?

5 Has your organization prioritized the risks and vulnerabilities that have been identified?

6 Does your risk analysis address both intentional and unintentional risks?

7 Does your organization periodically re-assess your vulnerabilities?

8 Does your organization re-evaluate your security procedures if there are security incidents?

9 Has your organization consistently applied the risk methodology when evaluating all implementation specifications?

Implementation Specification: Risk Management (REQUIRED)

Question

10 Does your organization have a systematic approach to risk mitigation based on your risk analysis?

11 Does your organization periodically review your risk management program?

Implementation Specification: Sanction Policy (REQUIRED)

Question

12 Does your organization have written sanction policies for security incidents?

13 Is there documented evidence that all personnel potentially affected by these sanctions are aware of the sanction policies?

Implementation Specification: Information System Activity Review (REQUIRED)

Using Management Reports

- Advising upper management
- Getting management support
- System admin buy in
- User buy in
- Create metrics
- Justify ROI
- Create support for implementation

Risk Assessment Tools

Raytheon

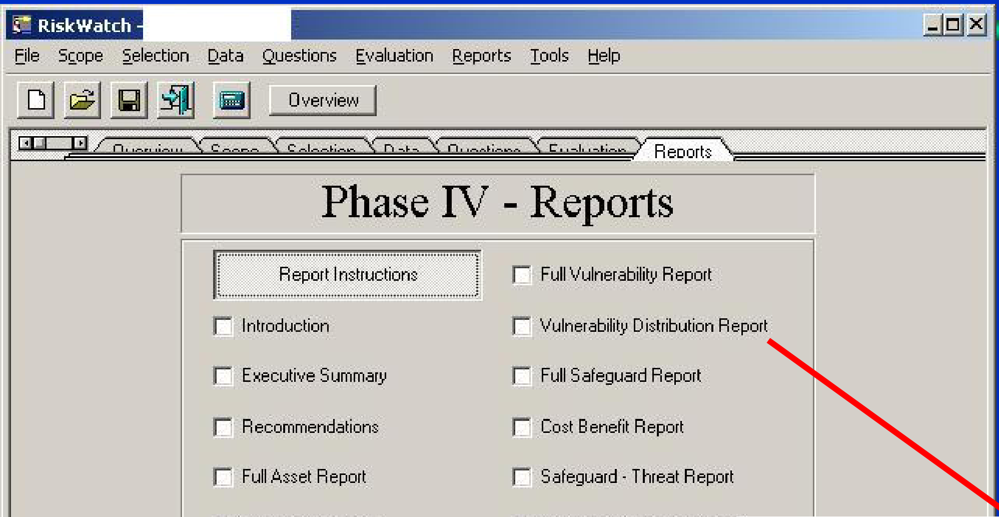
www.raytheon.com

HIPAA-Watch for Security™

Risk Assessment for the Healthcare Industry

www.riskwatch.com.com

Automated Process



Phase IV - Reports

Report Instructions

□ Introduction

□ Executive Summary

□ Recommendations

□ Full Asset Report

□ Summary by Asset

□ Full Threat Report

□ Summary by Threat

□ Full Vulnerability Report

□ Vulnerability Distribution Report

□ Full Safeguard Report

□ Cost Benefit Report

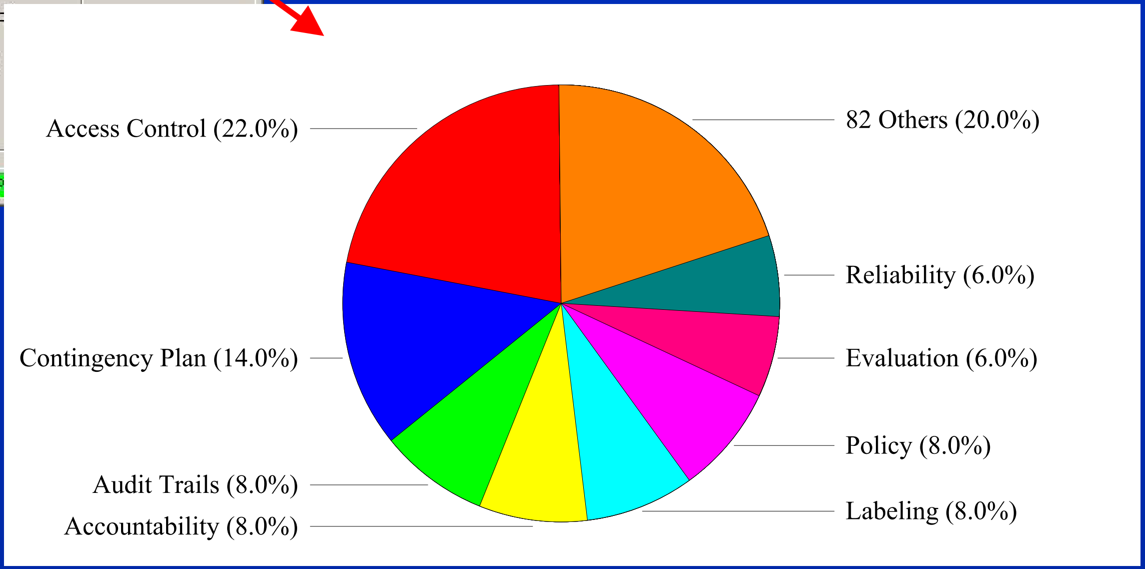
□ Safeguard - Threat Report

□ Audit Trail - Question Repo

□ Audit Trail - Respondents

□ Final Report

Vulnerability Distribution Report

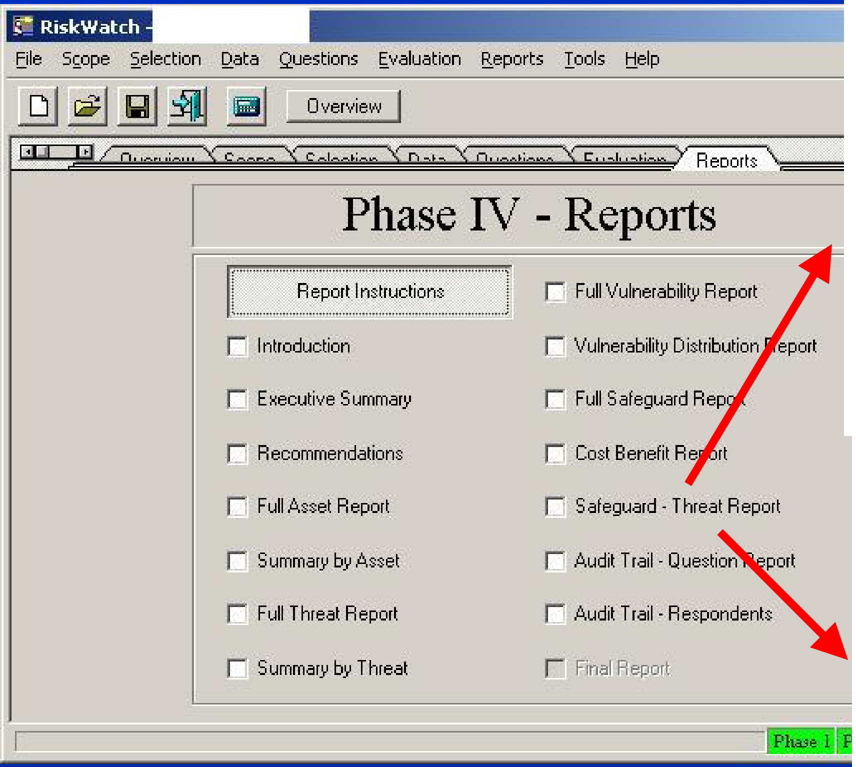


Phase IV: Reports

Automated Process

Phase IV: Reports

Implementation Costs



Phase IV - Reports

Report Instructions

☐ Introduction

☐ Executive Summary

☐ Recommendations

☐ Full Asset Report

☐ Summary by Asset

☐ Full Threat Report

☐ Summary by Threat

☐ Full Vulnerability Report

☐ Vulnerability Distribution Report

☐ Full Safeguard Report

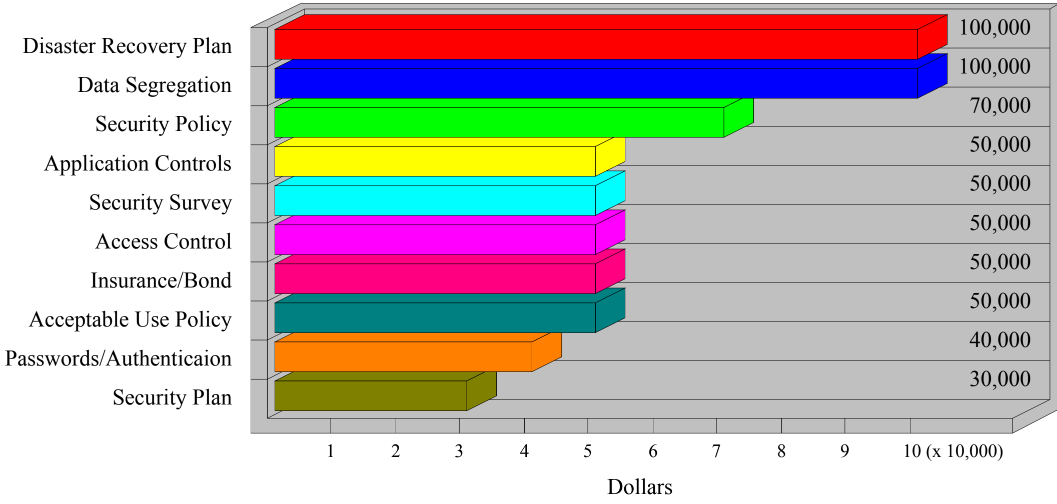
☐ Cost Benefit Report

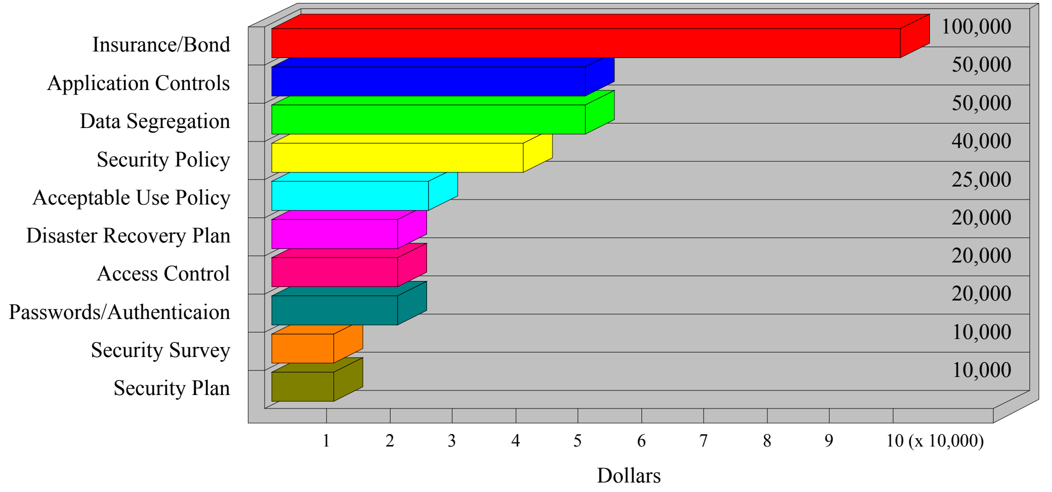
☐ Safeguard - Threat Report

☐ Audit Trail - Question Report

☐ Audit Trail - Respondents

☐ Final Report

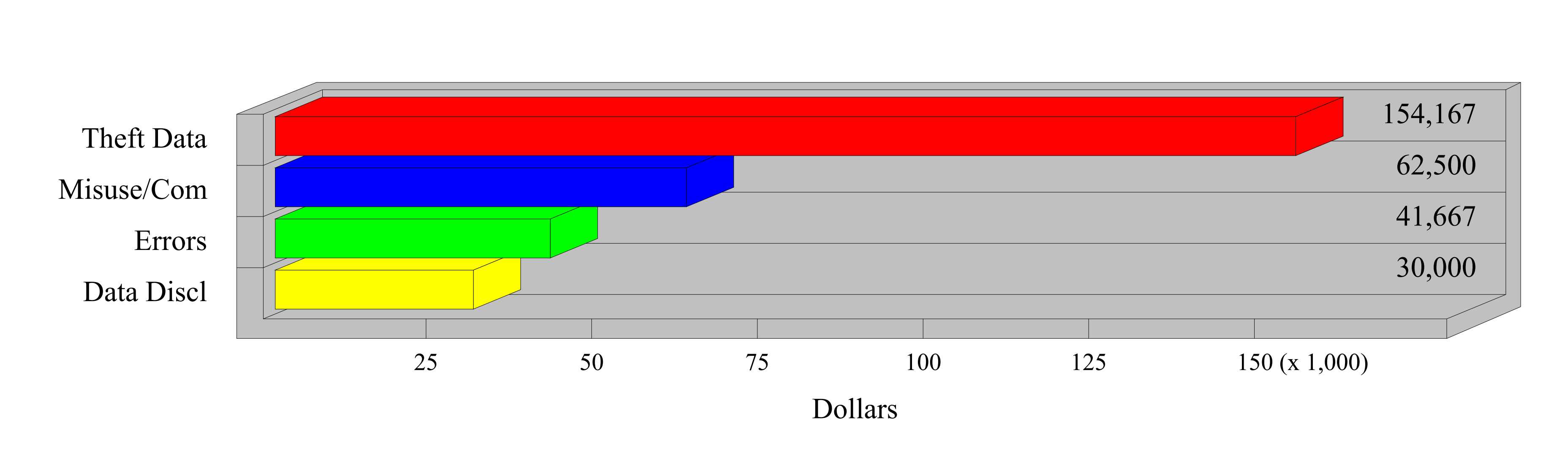




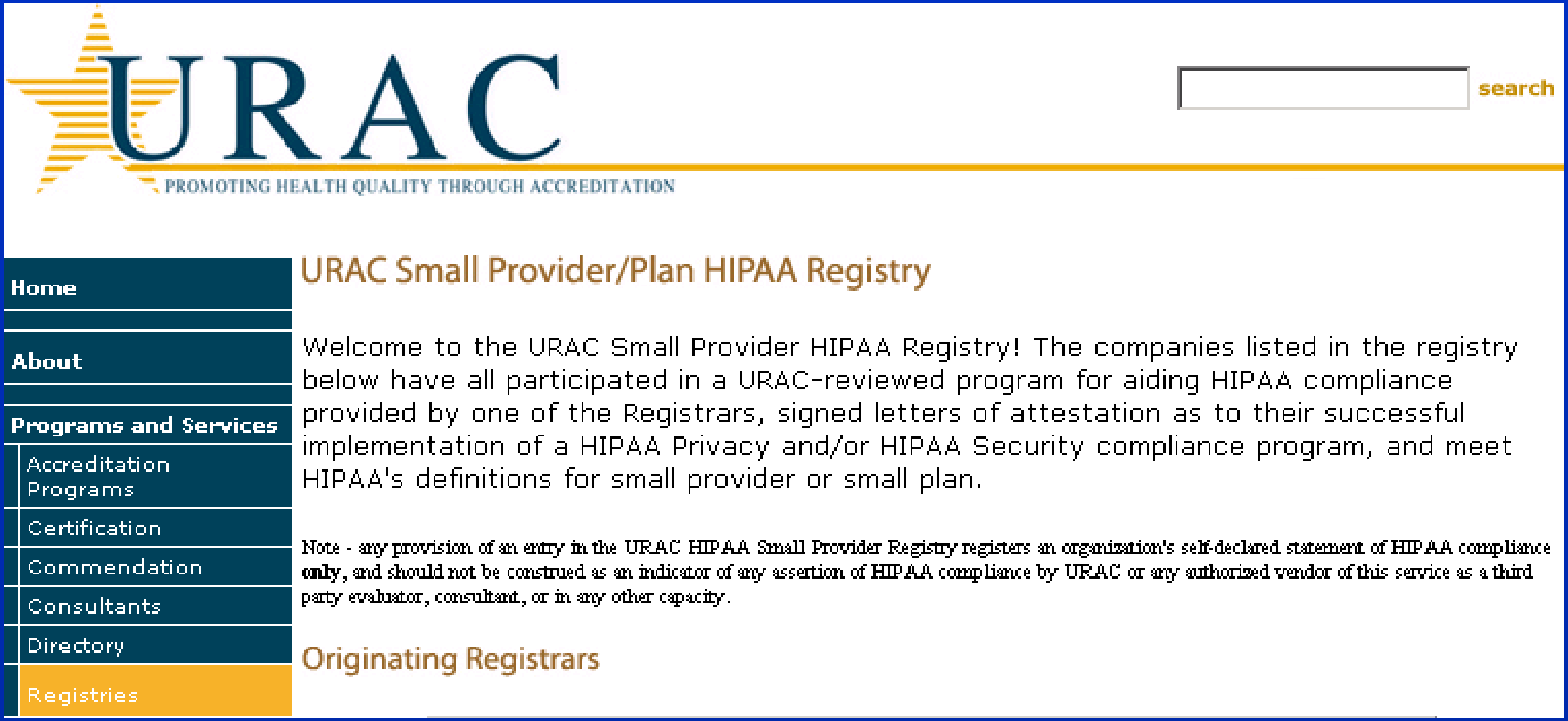
Maintenance Costs

Automated Process

Example Report: Annual Loss Expectancy



Security Compliance Registration



URAC Small Provider/Plan HIPAA Registry

Welcome to the URAC Small Provider HIPAA Registry! The companies listed in the registry below have all participated in a URAC-reviewed program for aiding HIPAA compliance provided by one of the Registrars, signed letters of attestation as to their successful implementation of a HIPAA Privacy and/or HIPAA Security compliance program, and meet HIPAA's definitions for small provider or small plan.

Note - any provision of an entry in the URAC HIPAA Small Provider Registry registers an organization's self-declared statement of HIPAA compliance **only**, and should not be construed as an indicator of any assertion of HIPAA compliance by URAC or any authorized vendor of this service as a third party evaluator, consultant, or in any other capacity.

Originating Registrars

www.urac.org

Coordinate with Other Laws, Regulations and Standards

Other Standards to Consider

- NIST Special Pub 800-30
  - “Risk Management Guide for Information Technology Systems”
- NIST Special Pub 800-37
  - “Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems”
- NIST Special Pub 800-53
  - “Minimum Security Controls for Federal Information Technology Systems”
- NIST Special Pub 800-53A
  - “Guidelines for the Selection and Specifications of Security Controls for Federal Information Systems”

Other Standards to Consider (cont.)

- NIST Special Pub 800-14
  - “Generally Accepted Principles and Practices for Securing Information Technology Systems”
- NIST Special Pub 800-16
  - “Information Technology Security Training Requirements: A Role- and Performance-based model”
- NIST Special Pub 800-18
  - “Security System”
- NIST Special Pub 800-34
  - “Business Contingency”

http://csrc.nist.gov/publications/nistpubs/

Other Standards to Consider (cont.)

- ISO/IEC 17799
- CMS Contractor Assessment Security Tool (CAST)
- Federal Information Processing Standards (FIPS)
  - Pub 199; Final Publication in December 2003
- Federal Information Security Management Act (FISMA)
- Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave^{SM}) CMU

Additional Resources

- www.nchica.org
  - Sample documents, tools, links
- www.wedi.org/snip
  - White papers, listserves, regional directory
- www.urac.org
  - Self-certification for privacy and security
  - Mapping of security standards
- www.cms.hhs.gov/hipaa/hipaa2/default.asp
  - Comprehensive site with FAQs and other tools

HIPAA EarlyView™ Tools Extenders

Jacob & Sundstrom	www.jasi.com
ParamoreConsultingInc.	www.paramoreconsulting.com
PARENTE RANDOLPH Accountants & Consultants	www.parentenet.com
Raytheon	www.raytheon.com

NCHICA

North Carolina Healthcare Information
and Communications Alliance, Inc.

www.nchica.org

Holt Anderson, Executive Director

holt@nchica.org

P.O. Box 13048, Research Triangle Park, NC 27709-3048

Voice: 919.558.9258 or 800.241.4486

Fax: 919.558.2198

Thank you!