Six+ Months to Go:

Tuning up for HIPAA Compliance – Tips of the Trade

Presented to:

Pre-Conference Symposia
The Ninth National HIPAA Summit

Holt Anderson, Executive Director

North Carolina Healthcare Information & Communications Alliance, Inc.

NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.

What keeps Privacy and Security Officials Awake at Night ?

What keeps Privacy and Security Officials Awake at Night ?

- Who is judging our effort?
  - Enforcement
- What don’t I know?
  - “Reasonably anticipated threats”
- How do we prove it?
  - Documentation
- What other Laws and Regulations apply?
  - Crosswalks
- Where do I get help?
  - Resources
- Why was I chosen?
  - ????

Compliance & Enforcement

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

CMS Office of HIPAA Standards:

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

Summary of HIPAA Privacy Rule Compliance Activities

- ❑ Received by HHS Office of Civil Rights (OCR)
- ❑ 7,577 complaints as of July 31, 2004.
- ❑ 57% have been closed, because either
  - ❑– Office for Civil Rights (OCR) lacks jurisdiction
  - ❑– There was no violation of the Privacy Rule
  - ❑– Complaint resolved through voluntary compliance

Summary of HIPAA Privacy Rule Compliance Activities (cont.)

- ❑ **Most frequent complaints**
  - ❑ **Impermissible use or disclosure**
  - ❑ **Lack of adequate safeguards**
  - ❑ **Refusal or failure to provide right of access**
  - ❑ **Disclosures not limited to "minimum necessary" standard**
  - ❑ **Failure to obtain individual's authorization, when required**
- ❑ **108 referrals to the Department of Justice (DOJ)**

OCR refers to the DOJ complaints involving the knowing disclosure or obtaining of protected health information in violation of the Privacy Rule.

Business Risks

- Loose 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

“Reasonably Anticipated Threats”

§ 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.

§ 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.

Security Case - Wireless

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 thousands 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

Security Case - Wireless

Holly Springs Man First In Nation Convicted Of Wireless Crime

Man Pleads Guilty To Hacking Into Patient Files

POSTED: 7:42 a.m. EST November 5, 2003

RALEIGH, N.C. -- Wireless Internet is becoming more and more popular, and with it come new ways for criminals to take advantage of others.

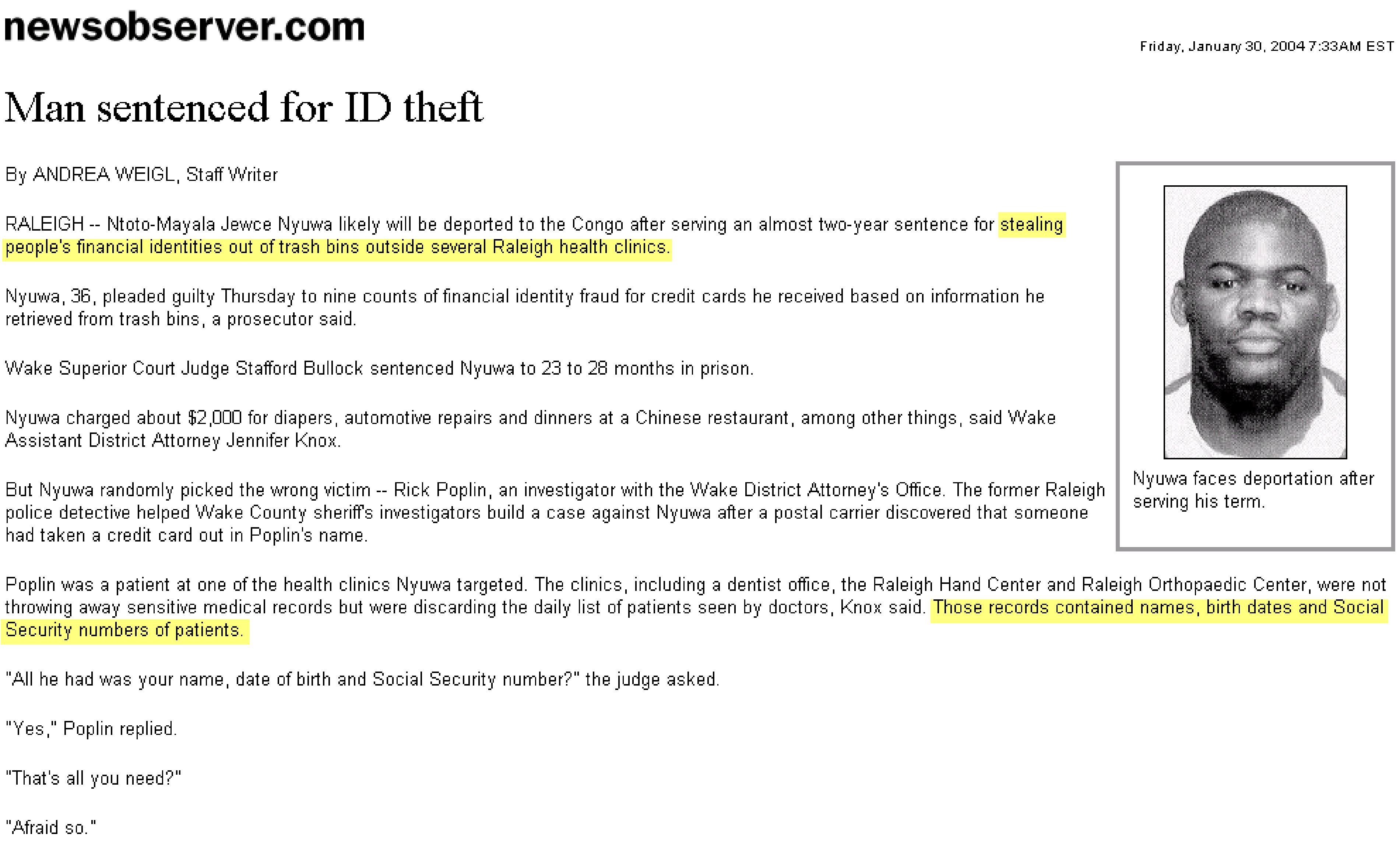
Clayton Dillard, 29, of Holly Springs, pleaded guilty to hacking into patient records at Wake Internal Medicine Consultants. Dillard said it was an experiment, but Raleigh police call it a crime.

Dillard said he broke the law to prove a point that confidential medical records are vulnerable to computer hackers.

Police said Dillard crossed the line by hacking into more than 2,000 patient files.

Dillard was sentenced to 18-months probation and ordered to pay $10,000 in fines.

Security Case – Identity Theft



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.

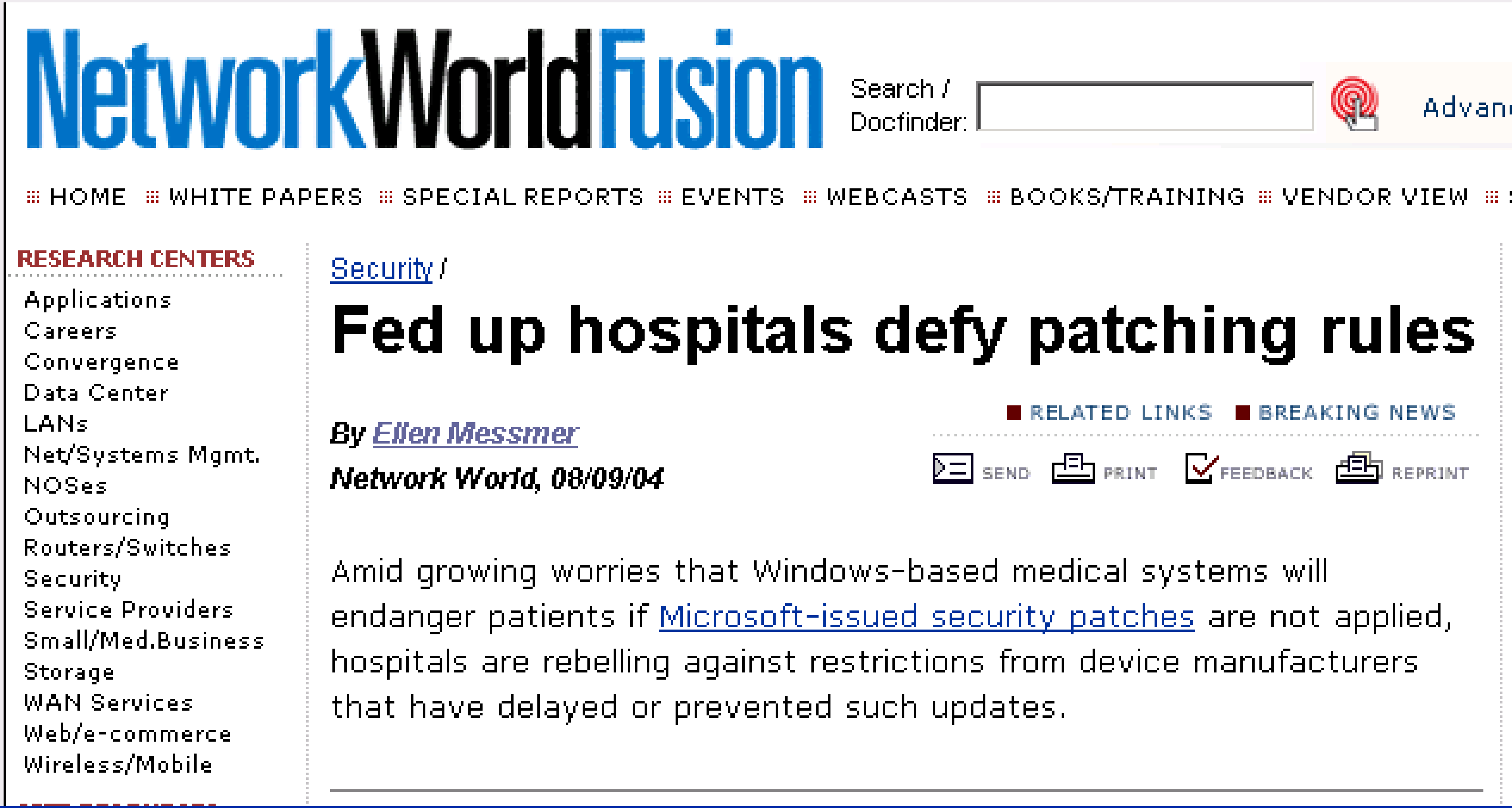
"All he had was your name, date of birth and Social Security number?" the judge asked.

"Yes," Poplin replied.

"That's all you need?"

"Afraid so."

Security Case – Patient Safety



Security /

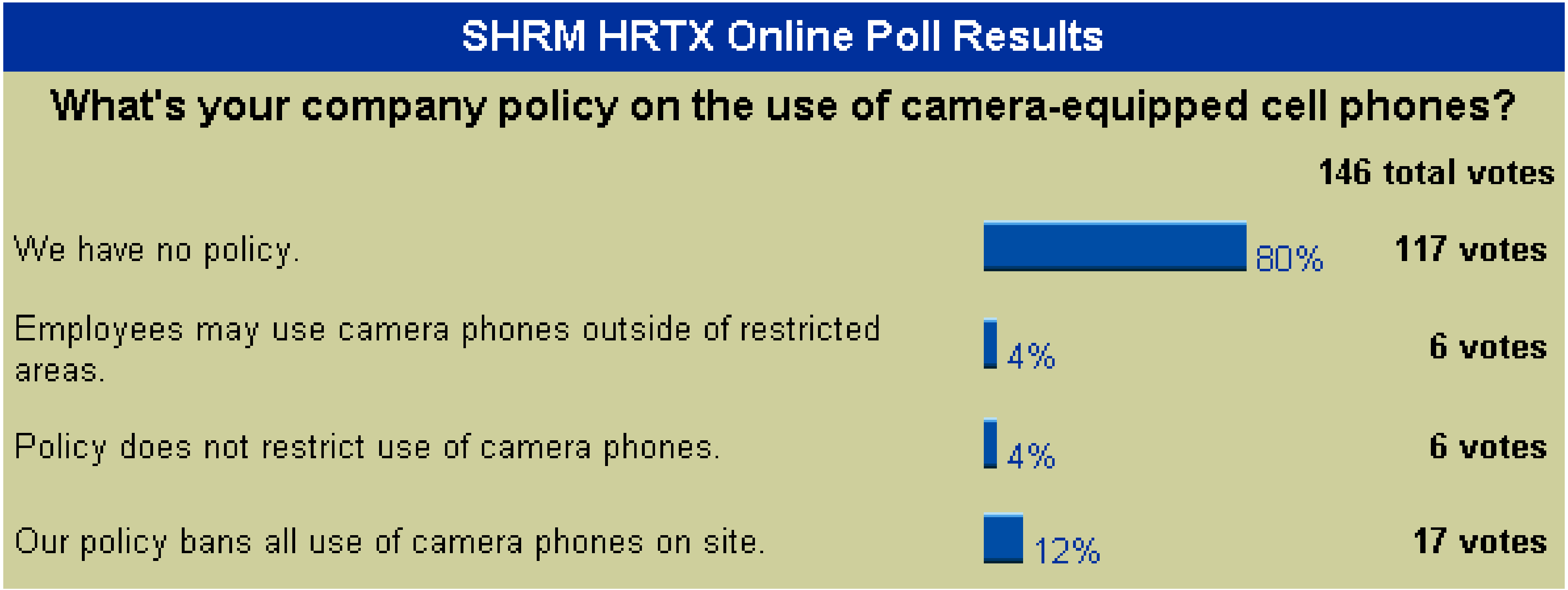
Fed up hospitals defy patching rules

By Ellen Messmer

Network World, 08/09/04

Amid growing worries that Windows-based medical systems will endanger patients if Microsoft-issued security patches are not applied, hospitals are rebelling against restrictions from device manufacturers that have delayed or prevented such updates.

“Reasonably Anticipated Threats”



SHRM HRTX Online Poll Results

What's your company policy on the use of camera-equipped cell phones?

146 total votes

We have no policy.	80%	**117 votes**
Employees may use camera phones outside of restricted areas.	4%	**6 votes**
Policy does not restrict use of camera phones.	4%	**6 votes**
Our policy bans all use of camera phones on site.	12%	**17 votes**

Reprinted with permission from the Society of Human Resources Management

Documentation

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
  - 6 Required, 0 Addressable

Organizational Requirements

- Business Associate Contracts
  - Tracking and monitoring
  - Re-negotiate and include Security provisions
  - ENSURE agents and subcontractors agree to implement reasonable and appropriate measures
- Group Health Plans
  - Creating separation with employment function
  - Reporting of security incidents
    - What to do about California law?

Policies and Procedures Documentation

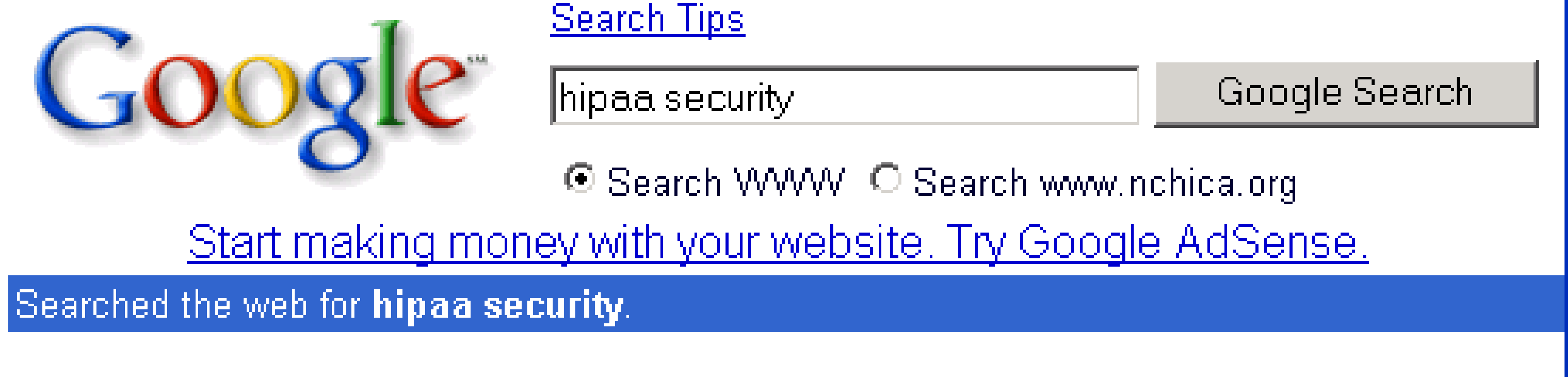
- Cataloging all policies and procedures
- Establishing time limit for retention
- Methods for making available
- Publishing updates

Updating and Maintaining Compliance

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

Resources

Are there resources ???

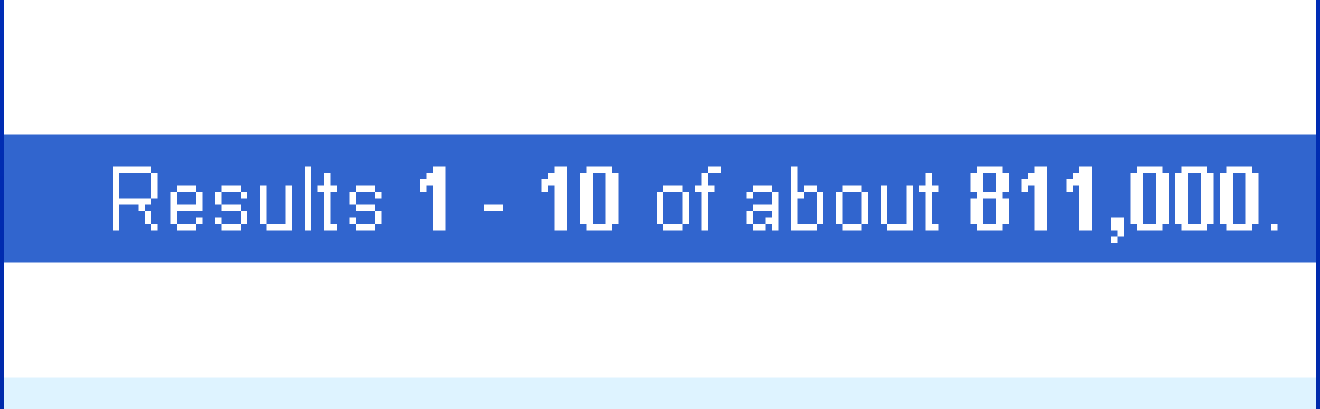


hipaa security

● Search WWW ○ Search www.nchica.org

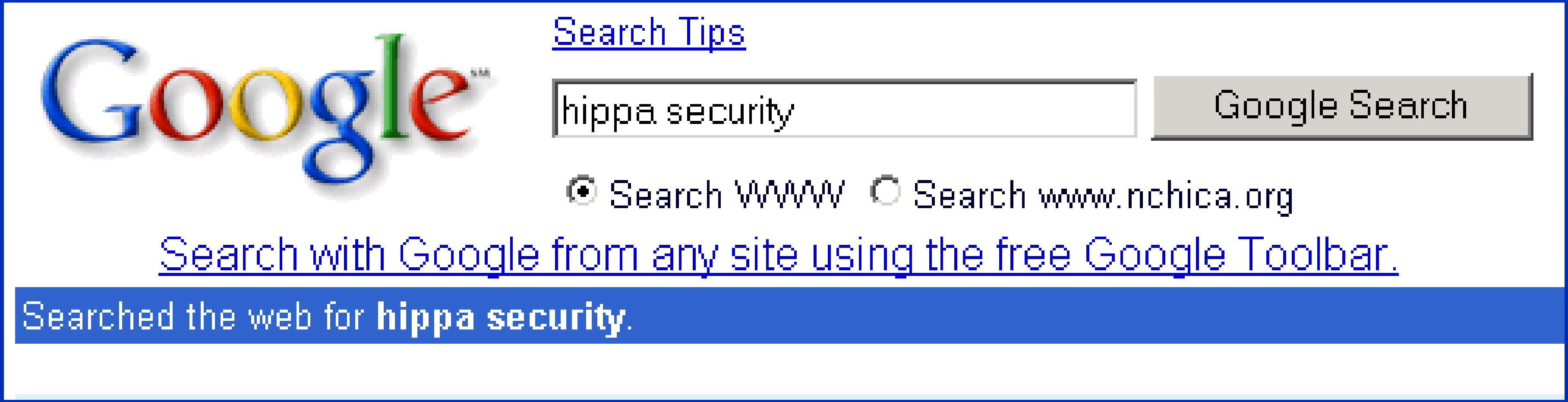
Start making money with your website. Try Google AdSense.

Searched the web for **hipaa security**.



Results **1** - **10** of about **811,000**.

Are there credible resources ???



Search Tips

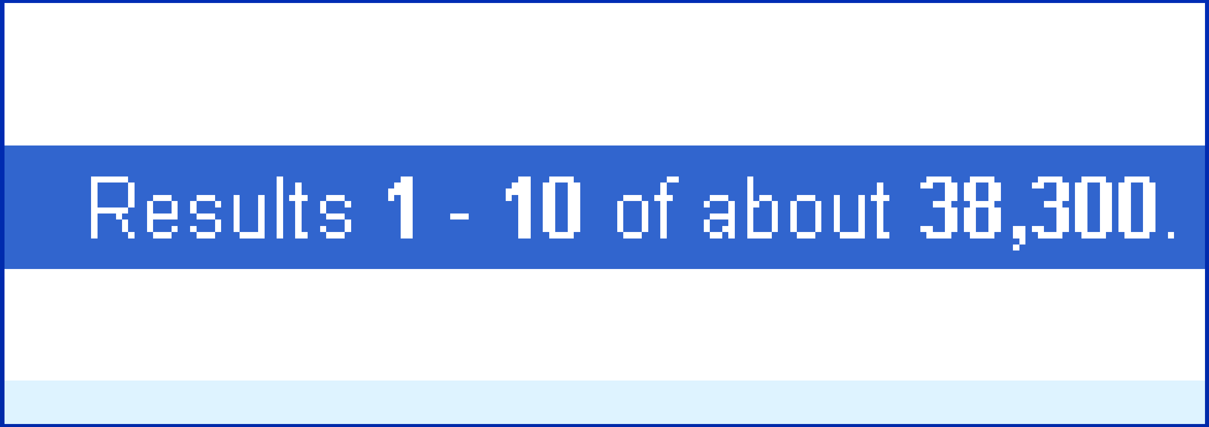
hippa security

Google Search

● Search WWW ○ Search www.nchica.org

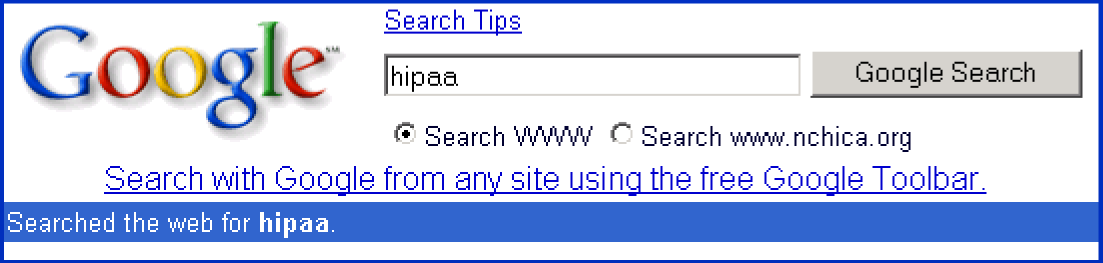
Search with Google from any site using the free Google Toolbar.

Searched the web for **hippa security**.



Results **1** - **10** of about **38,300**.

HIPAA & HIPPA

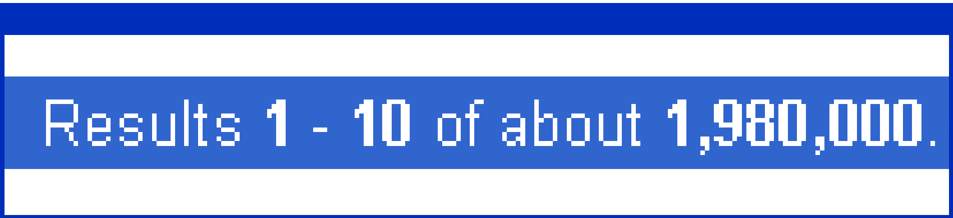


hipaa

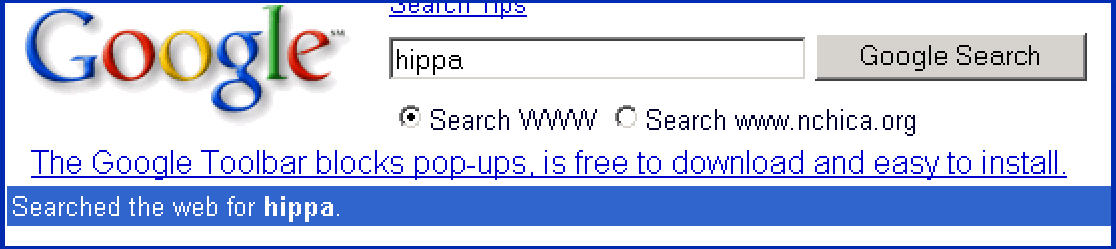
● Search WWW ○ Search www.nchica.org

Search with Google from any site using the free Google Toolbar.

Searched the web for **hipaa**.



Results **1** - **10** of about **1,980,000**.

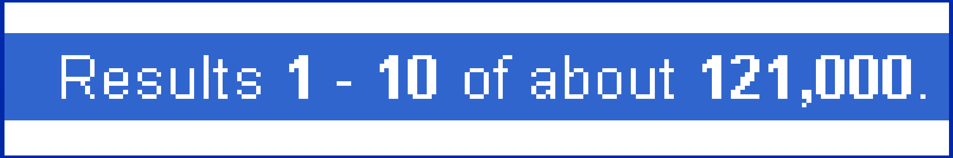


hippa

● Search WWW ○ Search www.nchica.org

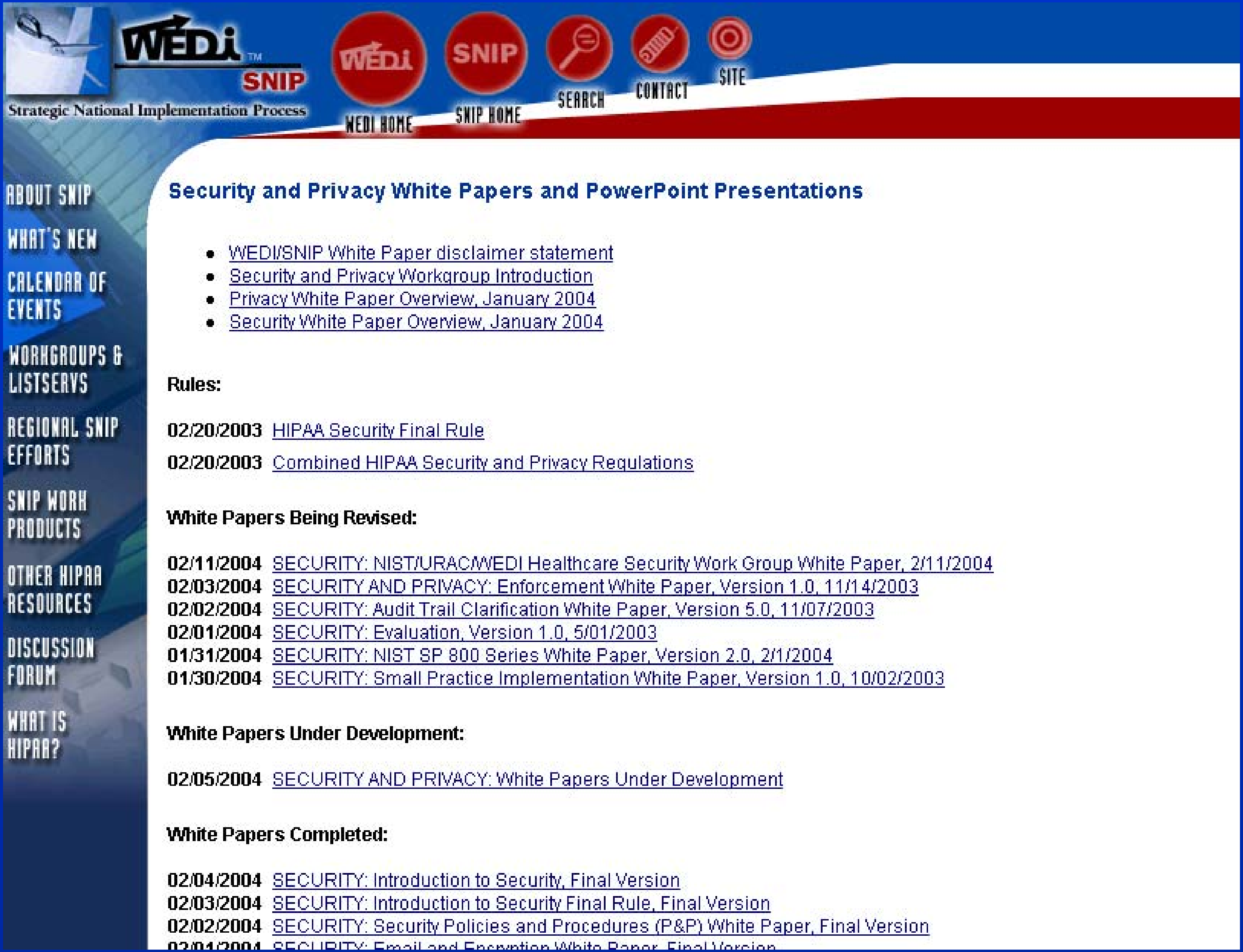
The Google Toolbar blocks pop-ups, is free to download and easy to install.

Searched the web for **hippa**.



Results **1** - **10** of about **121,000**.

Examples of Organizations, Tools, and Other Resources



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

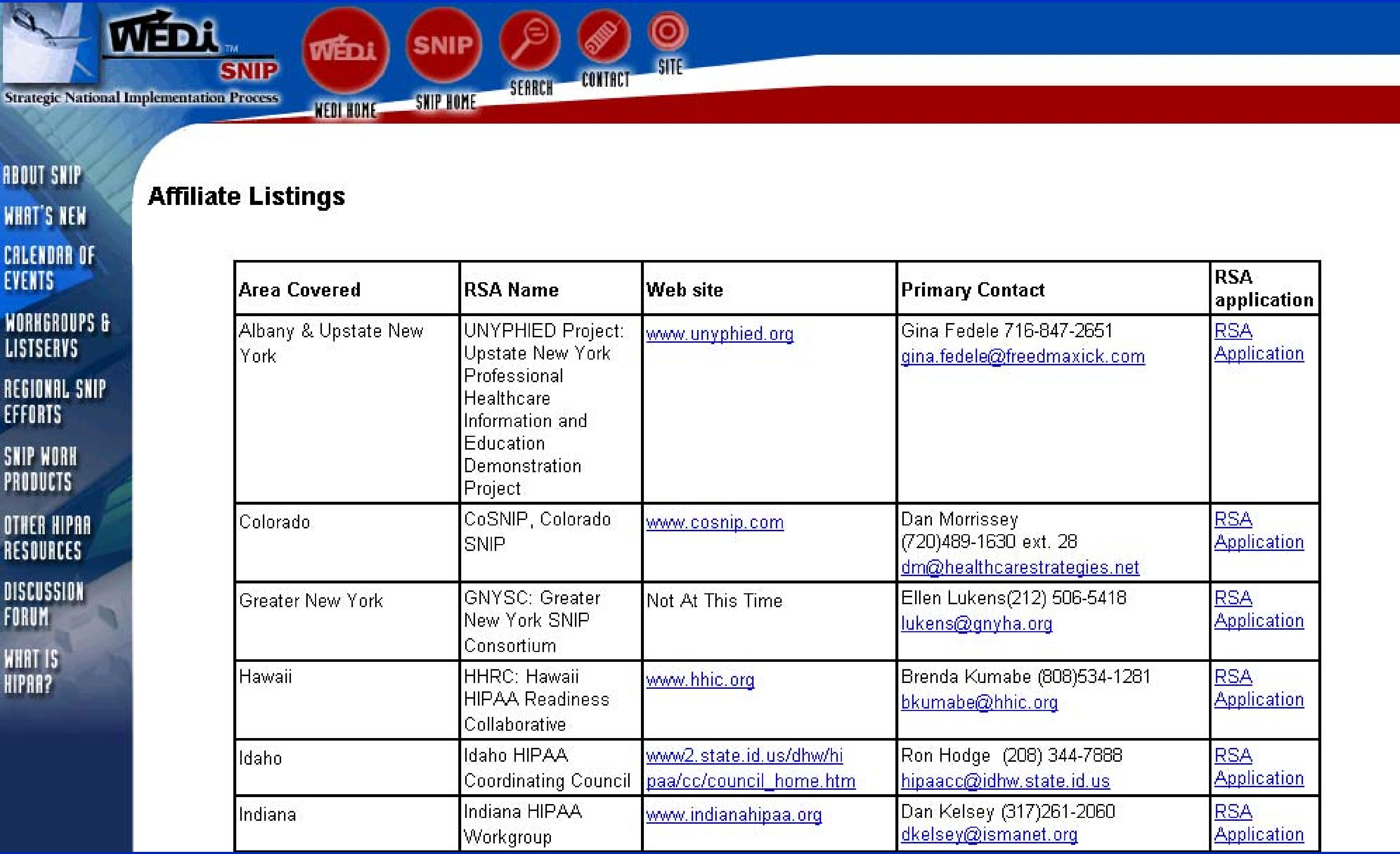
White Papers Under Development:

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

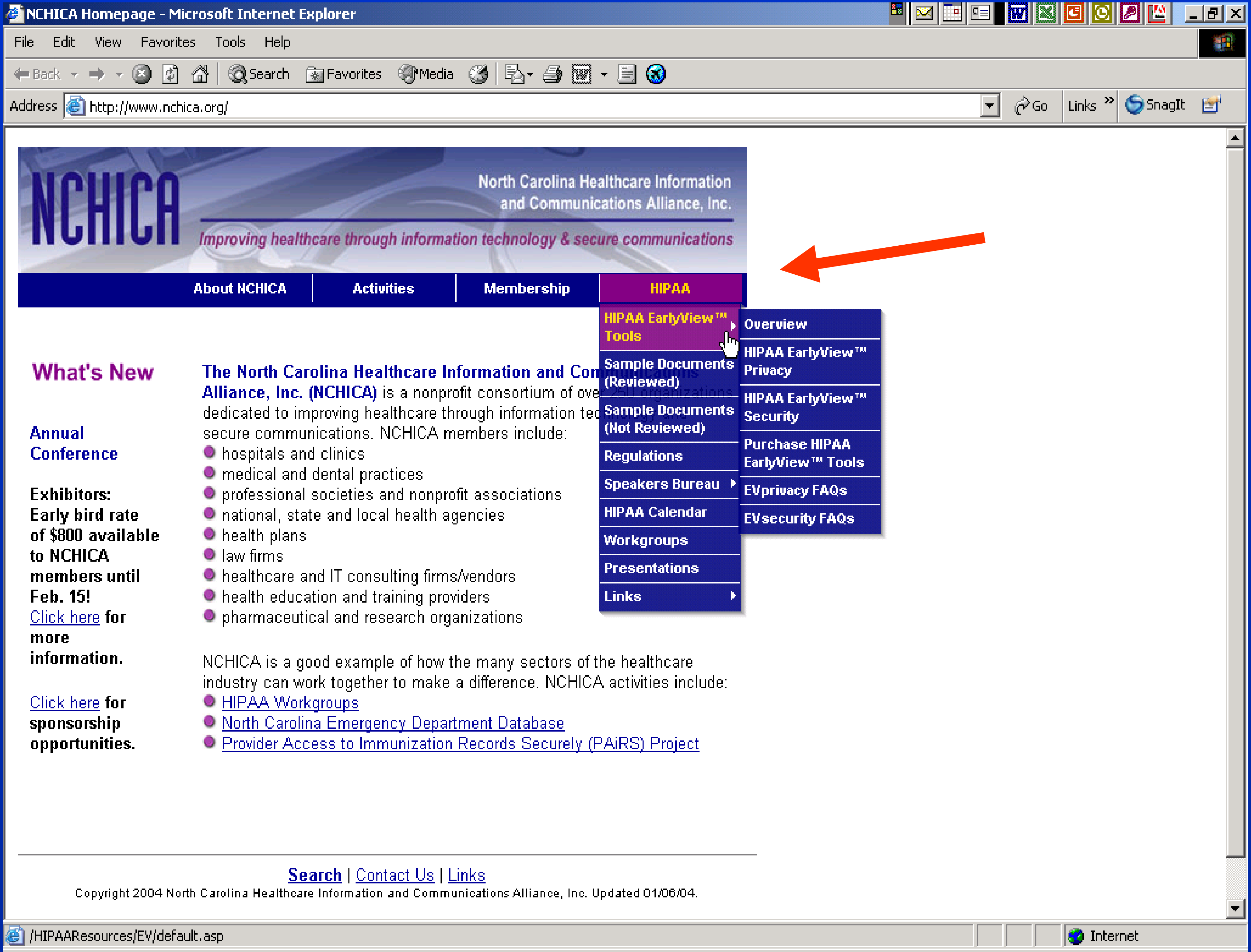
Resources Developed by NCHICA Members

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 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
Search | Contact Us | Links
/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.

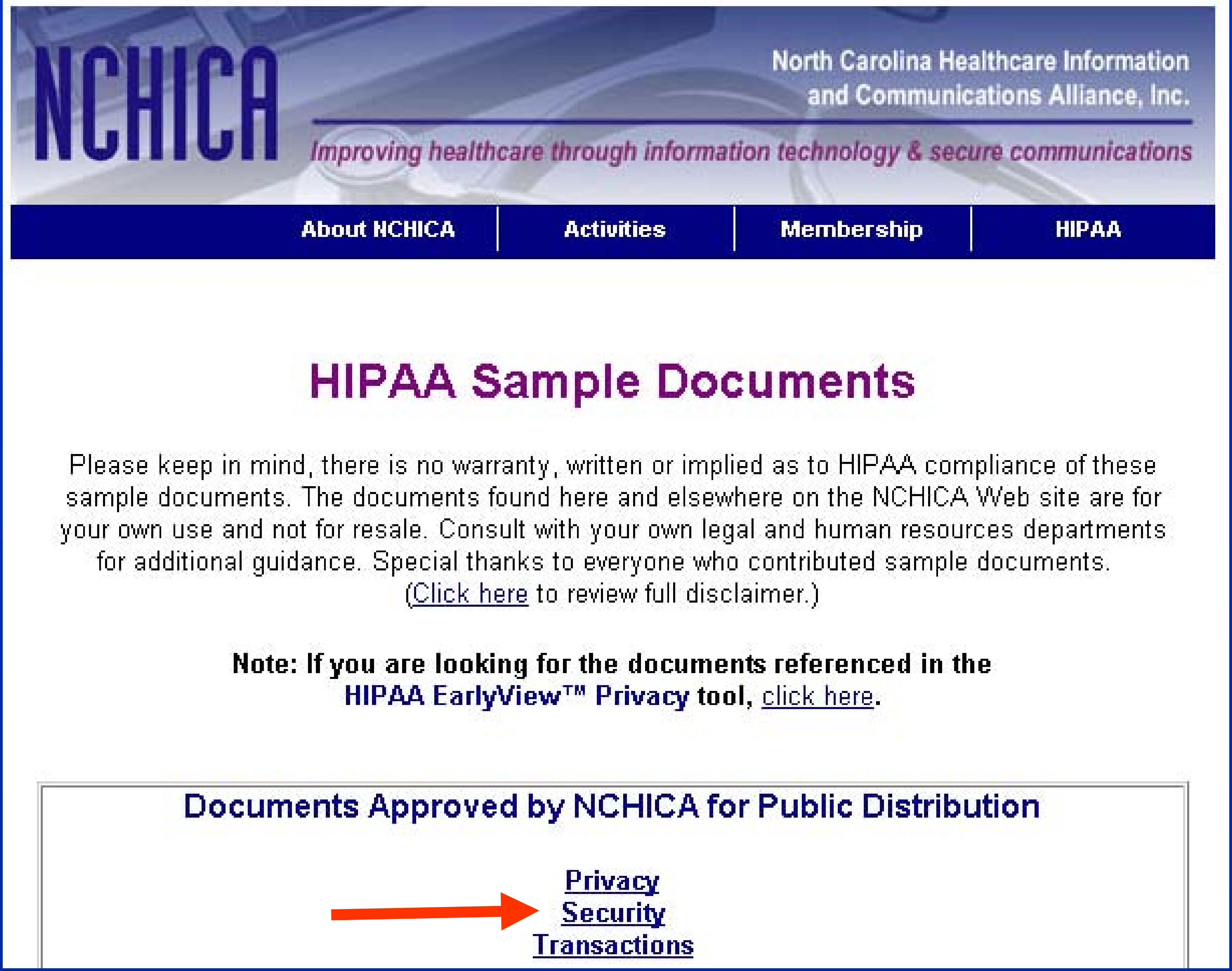
Click here for sponsorship opportunities.

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nonprofit consortium of over 250 organizations dedicated to improving healthcare through information technology and 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


NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.
Improving healthcare through information technology & secure communications
About NCHICA
Activities
Membership
HIPAA

HIPAA Sample Documents

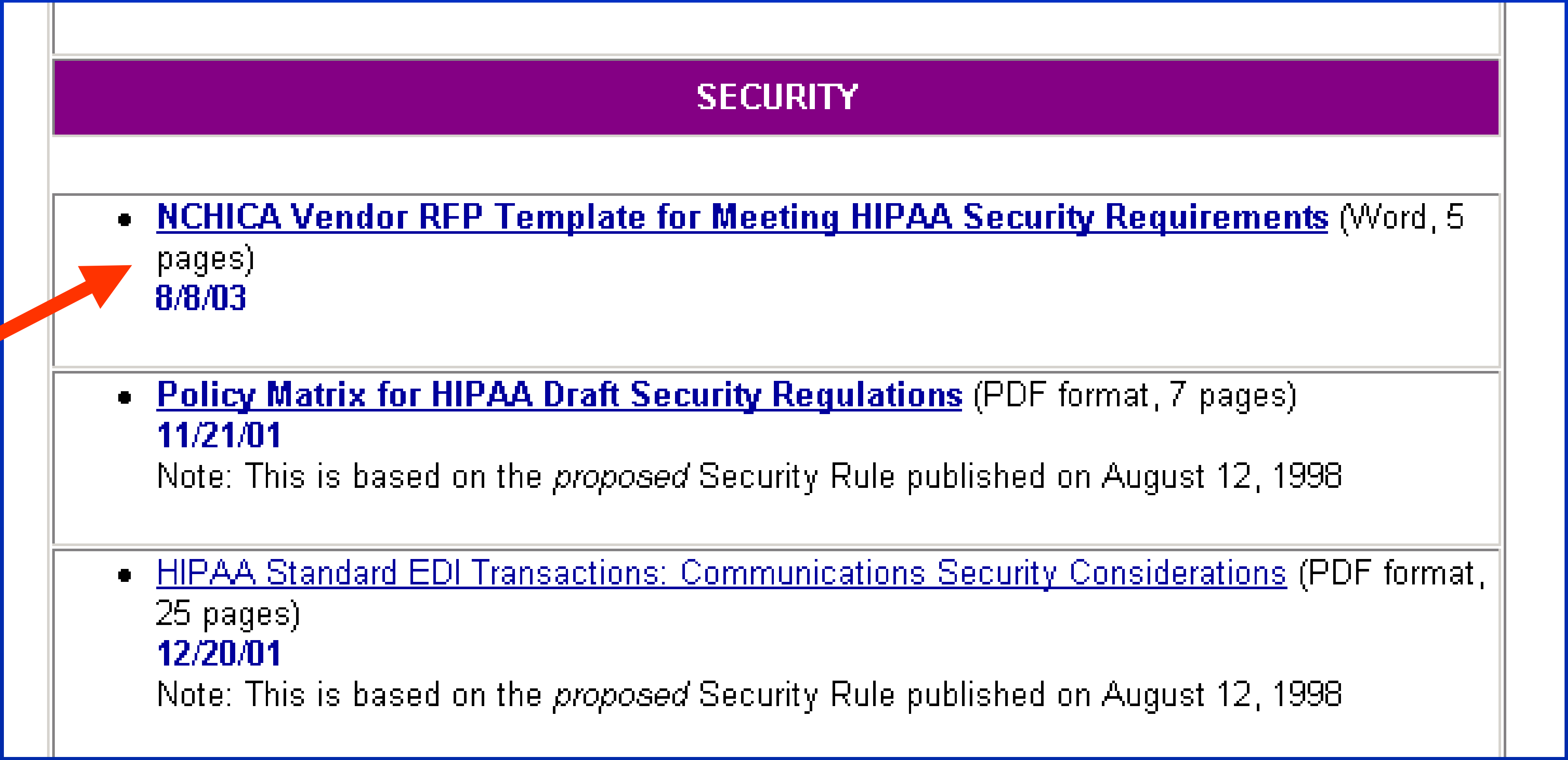
Please keep in mind, there is no warranty, written or implied as to HIPAA compliance of these sample documents. The documents found here and elsewhere on the NCHICA Web site are for your own use and not for resale. Consult with your own legal and human resources departments for additional guidance. Special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

Sample Documents – Vendor Template



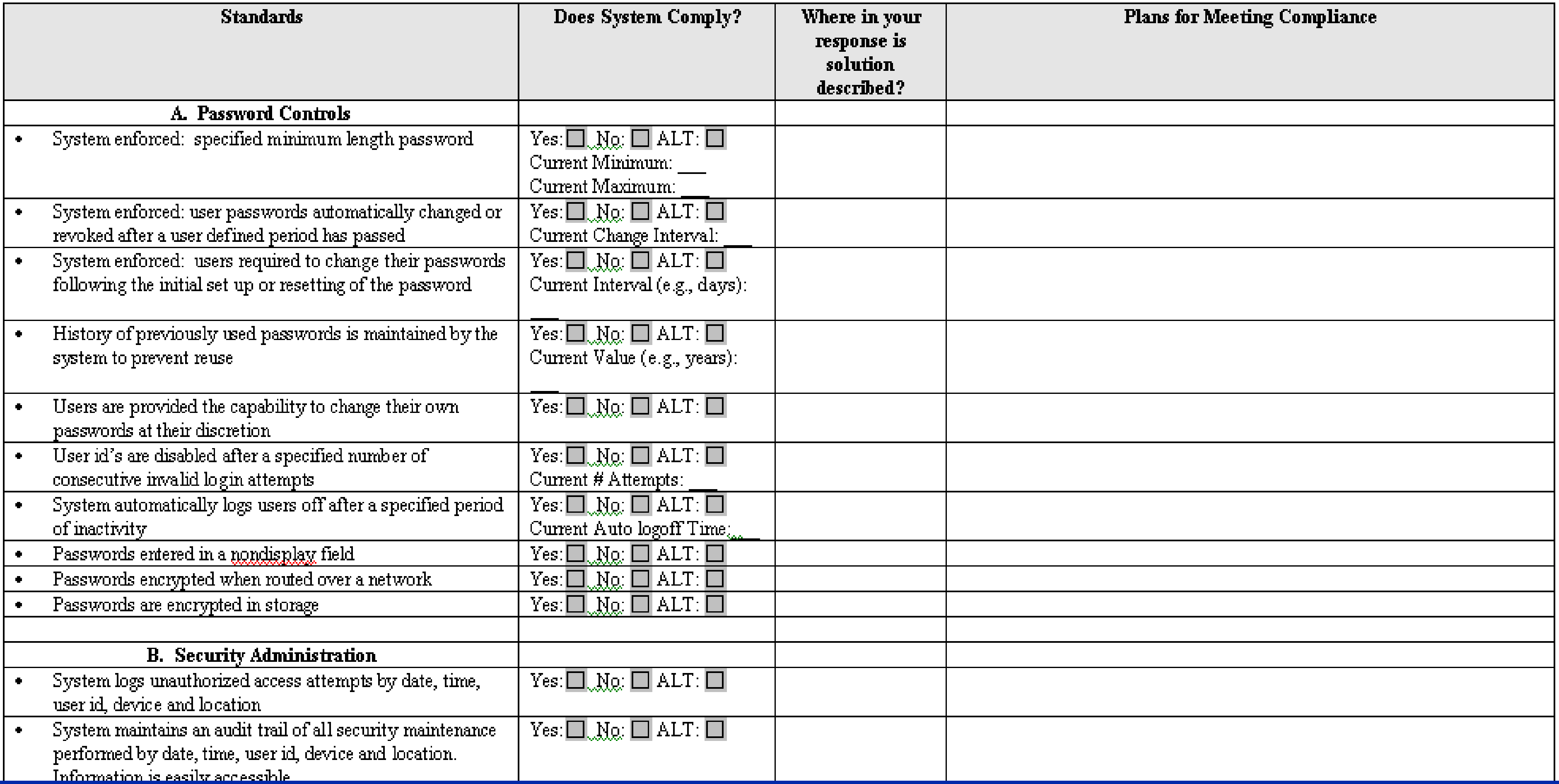
SECURITY

- NCHICA Vendor RFP Template for Meeting HIPAA Security Requirements (Word, 5 pages)
  8/8/03

- Policy Matrix for HIPAA Draft Security Regulations (PDF format, 7 pages)
  11/21/01
  Note: This is based on the *proposed* Security Rule published on August 12, 1998

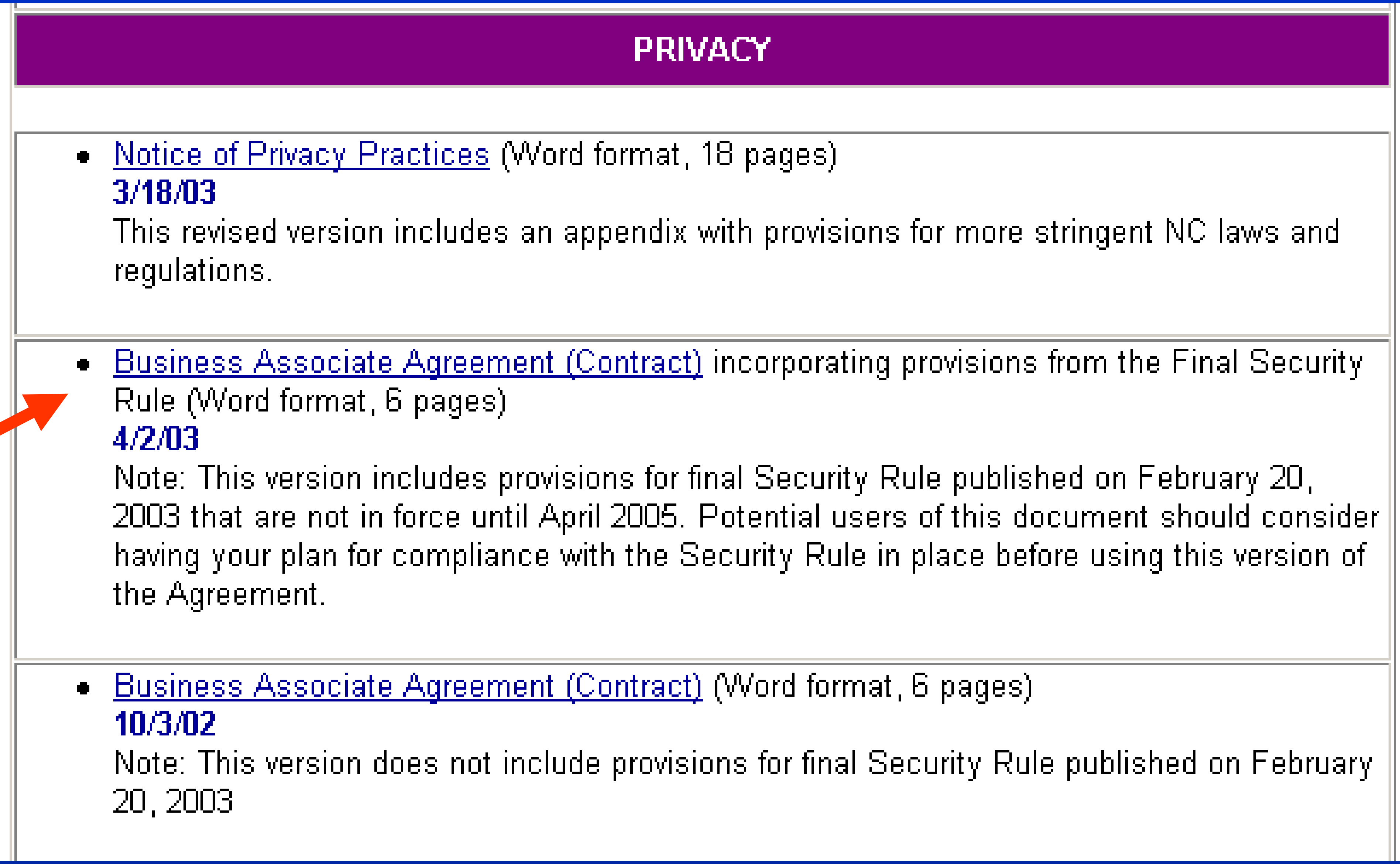
- HIPAA Standard EDI Transactions: Communications Security Considerations (PDF format, 25 pages)
  12/20/01
  Note: This is based on the *proposed* Security Rule published on August 12, 1998

NCHICA Vendor RFP Template



Standards	Does System Comply?	Where in your response is solution described?	Plans for Meeting Compliance
A. Password Controls			
• System enforced: specified minimum length password	Yes: □ No: □ ALT: □ Current Minimum: ___ Current Maximum: ___		
• System enforced: user passwords automatically changed or revoked after a user defined period has passed	Yes: □ No: □ ALT: □ Current Change Interval: ___		
• System enforced: users required to change their passwords following the initial set up or resetting of the password	Yes: □ No: □ ALT: □ Current Interval (e.g., days): ___		
• History of previously used passwords is maintained by the system to prevent reuse	Yes: □ No: □ ALT: □ Current Value (e.g., years): ___		
• Users are provided the capability to change their own passwords at their discretion	Yes: □ No: □ ALT: □		
• User id's are disabled after a specified number of consecutive invalid login attempts	Yes: □ No: □ ALT: □ Current # Attempts: ___		
• System automatically logs users off after a specified period of inactivity	Yes: □ No: □ ALT: □ Current Auto logoff Time: ___		
• Passwords entered in a nondisplay field	Yes: □ No: □ ALT: □		
• Passwords encrypted when routed over a network	Yes: □ No: □ ALT: □		
• Passwords are encrypted in storage	Yes: □ No: □ ALT: □		
B. Security Administration			
• System logs unauthorized access attempts by date, time, user id, device and location	Yes: □ No: □ ALT: □		
• System maintains an audit trail of all security maintenance performed by date, time, user id, device and location. Information is easily accessible	Yes: □ No: □ ALT: □		

Sample Documents – BAA w/ Security

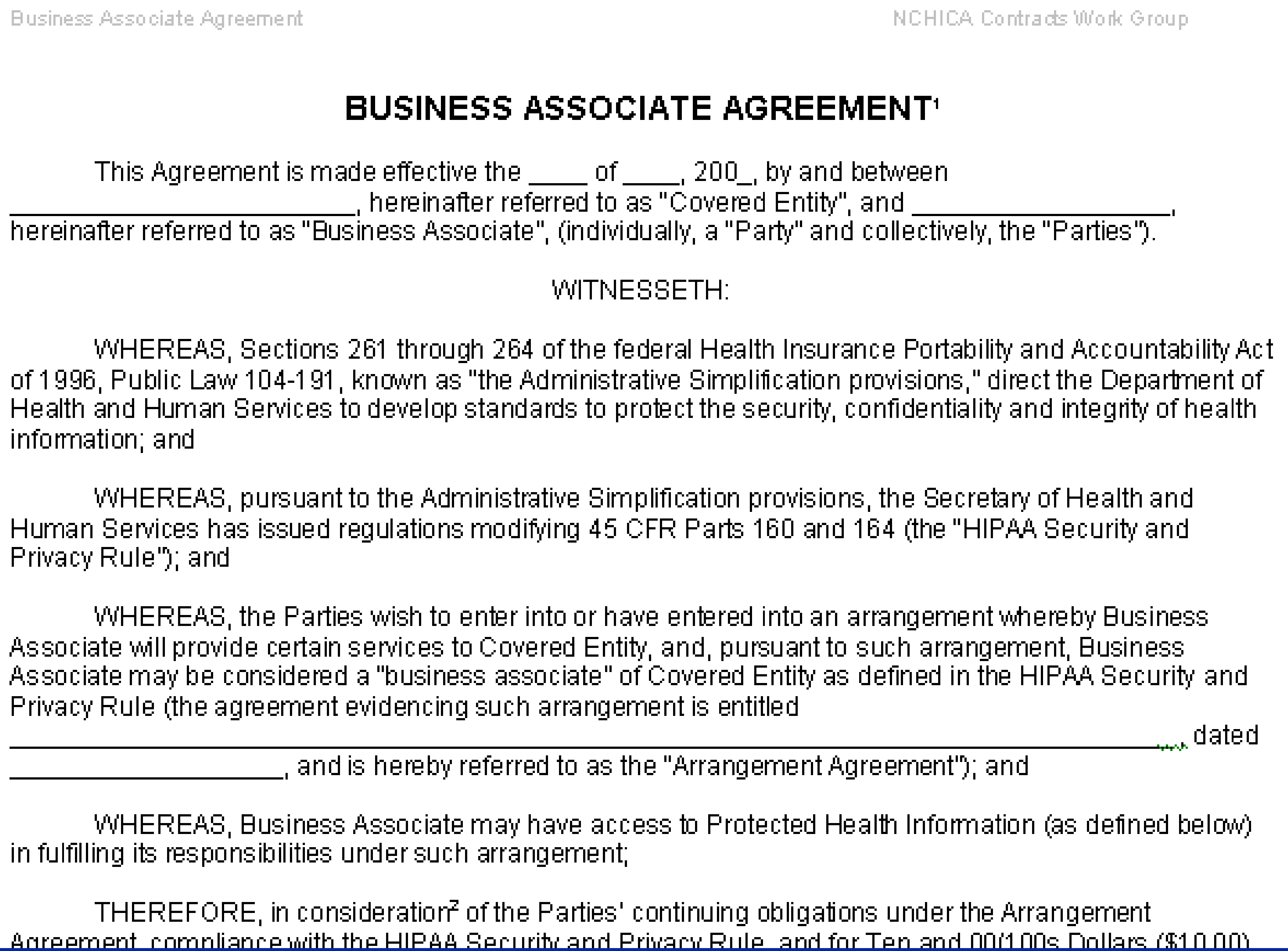


PRIVACY

- Notice of Privacy Practices (Word format, 18 pages)
  3/18/03
  This revised version includes an appendix with provisions for more stringent NC laws and regulations.

- Business Associate Agreement (Contract) incorporating provisions from the Final Security Rule (Word format, 6 pages)
  4/2/03
  Note: This version includes provisions for final Security Rule published on February 20, 2003 that are not in force until April 2005. Potential users of this document should consider having your plan for compliance with the Security Rule in place before using this version of the Agreement.

- Business Associate Agreement (Contract) (Word format, 6 pages)
  10/3/02
  Note: This version does not include provisions for final Security Rule published on February 20, 2003



BUSINESS ASSOCIATE AGREEMENT[1]

This Agreement is made effective the ____ of ____, 200_, by and between ____________________________, hereinafter referred to as "Covered Entity", and _____________________, hereinafter referred to as "Business Associate", (individually, a "Party" and collectively, the "Parties").

WITNESSETH:

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and

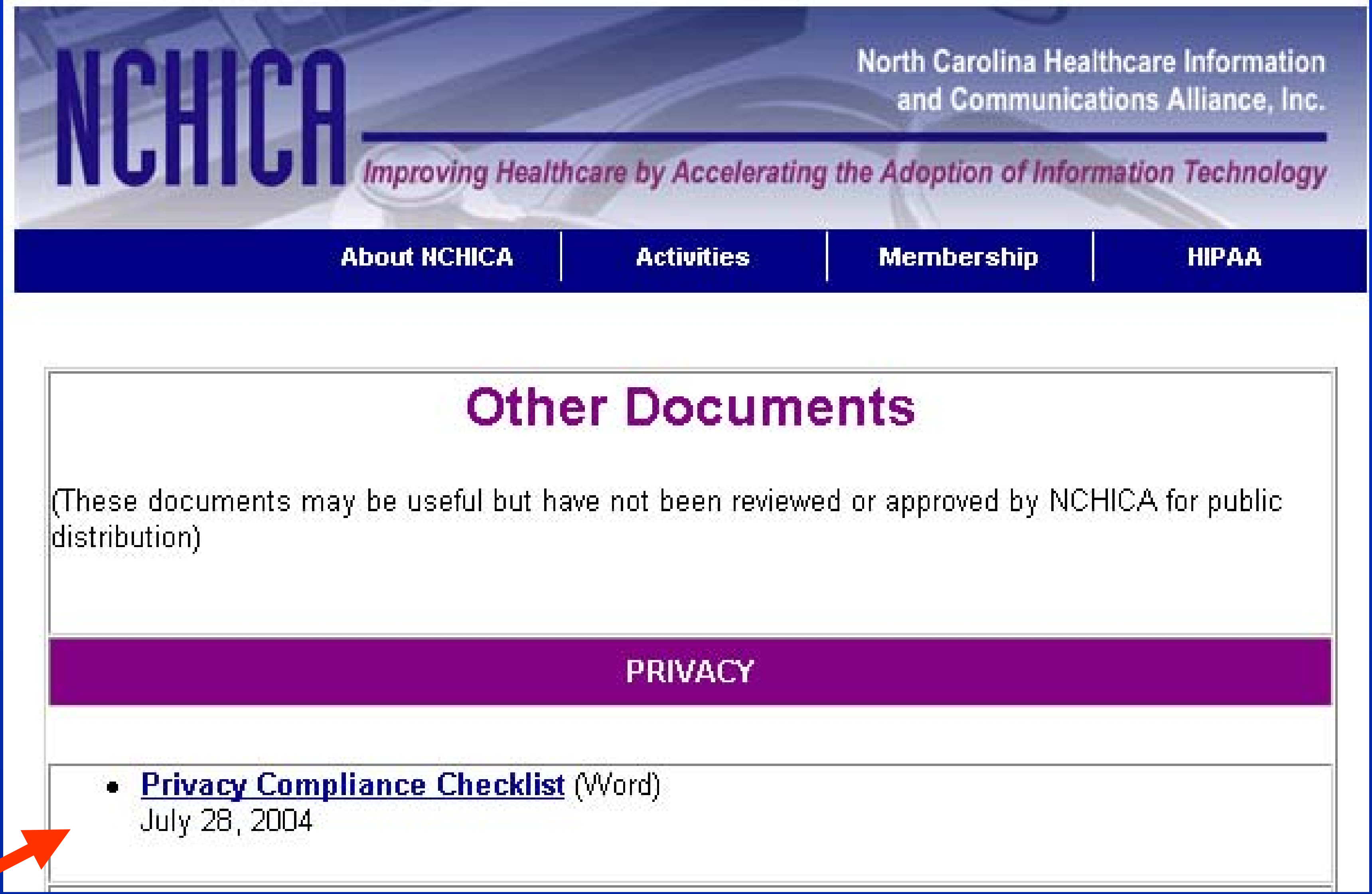
WHEREAS, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services has issued regulations modifying 45 CFR Parts 160 and 164 (the "HIPAA Security and Privacy Rule"); and

WHEREAS, the Parties wish to enter into or have entered into an arrangement whereby Business Associate will provide certain services to Covered Entity, and, pursuant to such arrangement, Business Associate may be considered a "business associate" of Covered Entity as defined in the HIPAA Security and Privacy Rule (the agreement evidencing such arrangement is entitled ____, dated ______________________, and is hereby referred to as the "Arrangement Agreement"); and

WHEREAS, Business Associate may have access to Protected Health Information (as defined below) in fulfilling its responsibilities under such arrangement;

THEREFORE, in consideration[2] of the Parties' continuing obligations under the Arrangement Agreement, compliance with the HIPAA Security and Privacy Rule, and for Ten and 00/100s Dollars ($10.00)

Sample Documents – Privacy Compliance Check List w/ Security



NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.
Improving Healthcare by Accelerating the Adoption of Information Technology
About NCHICA
Activities
Membership
HIPAA

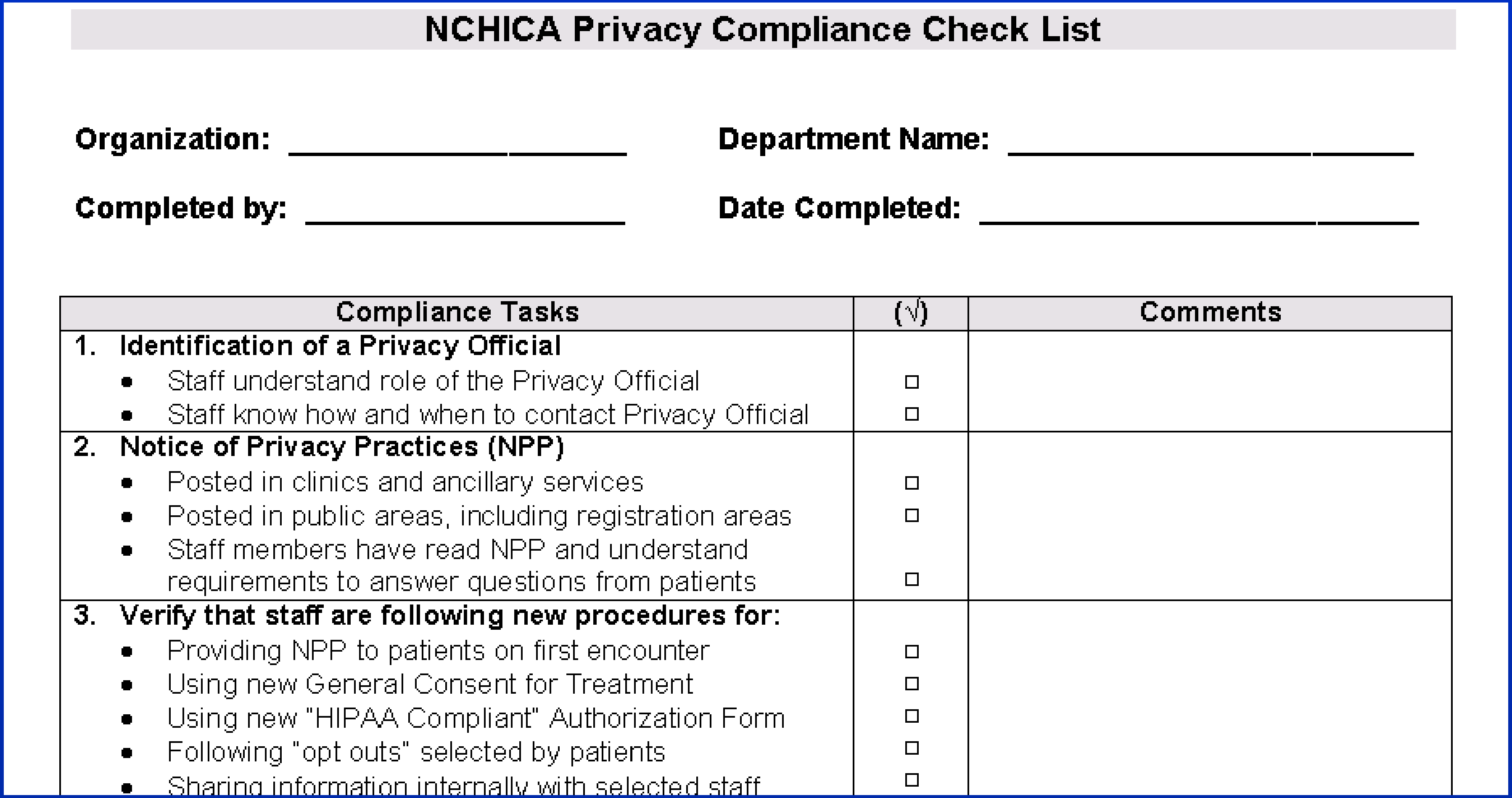
Other Documents

(These documents may be useful but have not been reviewed or approved by NCHICA for public distribution)

PRIVACY

- Privacy Compliance Checklist (Word)
  July 28, 2004

Privacy Compliance Checklist



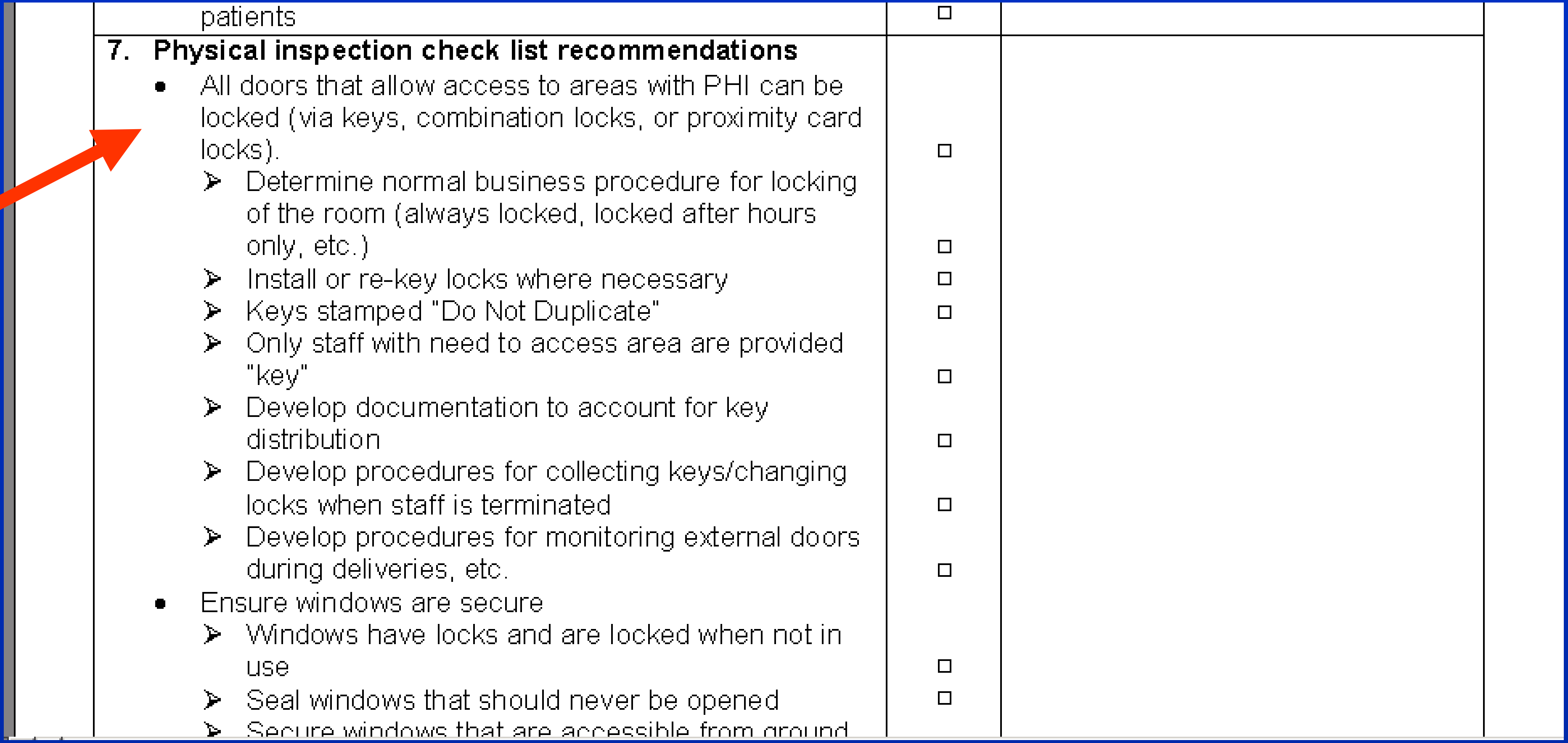
NCHICA Privacy Compliance Check List

Organization: ____________________ **Department Name:** ________________________

Completed by: ___________________ **Date Completed:** __________________________

Compliance Tasks	(√)	Comments
1. **Identification of a Privacy Official**		
• Staff understand role of the Privacy Official	□	
• Staff know how and when to contact Privacy Official	□	
2. **Notice of Privacy Practices (NPP)**		
• Posted in clinics and ancillary services	□	
• Posted in public areas, including registration areas	□	
• Staff members have read NPP and understand requirements to answer questions from patients	□	
3. **Verify that staff are following new procedures for:**		
• Providing NPP to patients on first encounter	□	
• Using new General Consent for Treatment	□	
• Using new "HIPAA Compliant" Authorization Form	□	
• Following "opt outs" selected by patients	□	
• Sharing information internally with selected staff	□	

Privacy Compliance Checklist



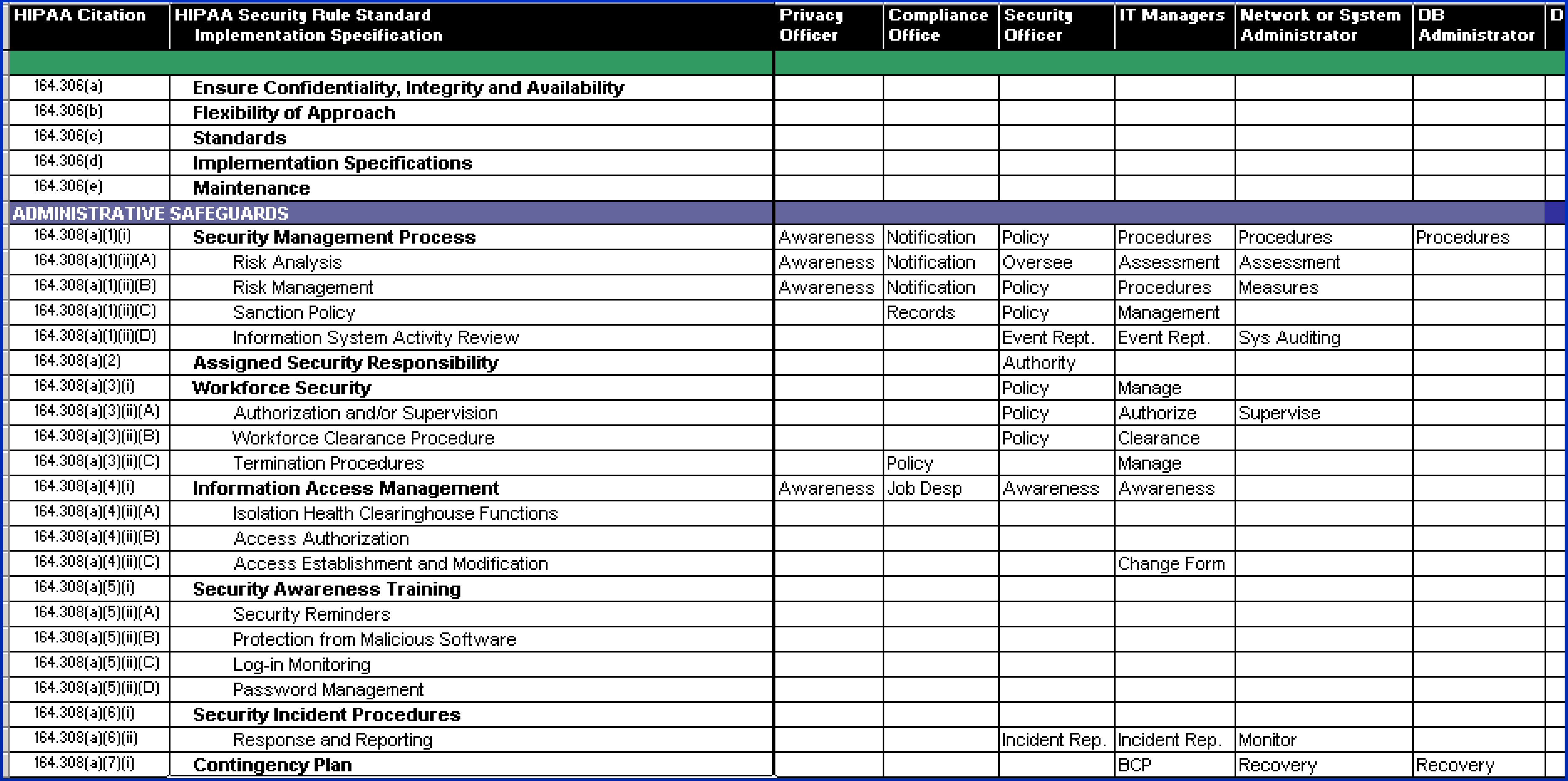
patients	□	
7. Physical inspection check list recommendations		
• All doors that allow access to areas with PHI can be locked (via keys, combination locks, or proximity card locks).	□	
➢ Determine normal business procedure for locking of the room (always locked, locked after hours only, etc.)	□	
➢ Install or re-key locks where necessary	□	
➢ Keys stamped "Do Not Duplicate"	□	
➢ Only staff with need to access area are provided "key"	□	
➢ Develop documentation to account for key distribution	□	
➢ Develop procedures for collecting keys/changing locks when staff is terminated	□	
➢ Develop procedures for monitoring external doors during deliveries, etc.	□	
• Ensure windows are secure		
➢ Windows have locks and are locked when not in use	□	
➢ Seal windows that should never be opened	□	
➢ Secure windows that are accessible from ground		

Compliance Checklist Spreadsheet

- Free tool developed by NC Division of Mental Health / Developmental Disabilities / Substance Abuse Services (MH/DD/SAS)
- Spreadsheet checklist to assist groups within agency and others to understand and plan for HIPAA Security compliance
- Checklist is being made available free to the public through NCHICA and from them directly
- Will be published on NCHICA Web site shortly

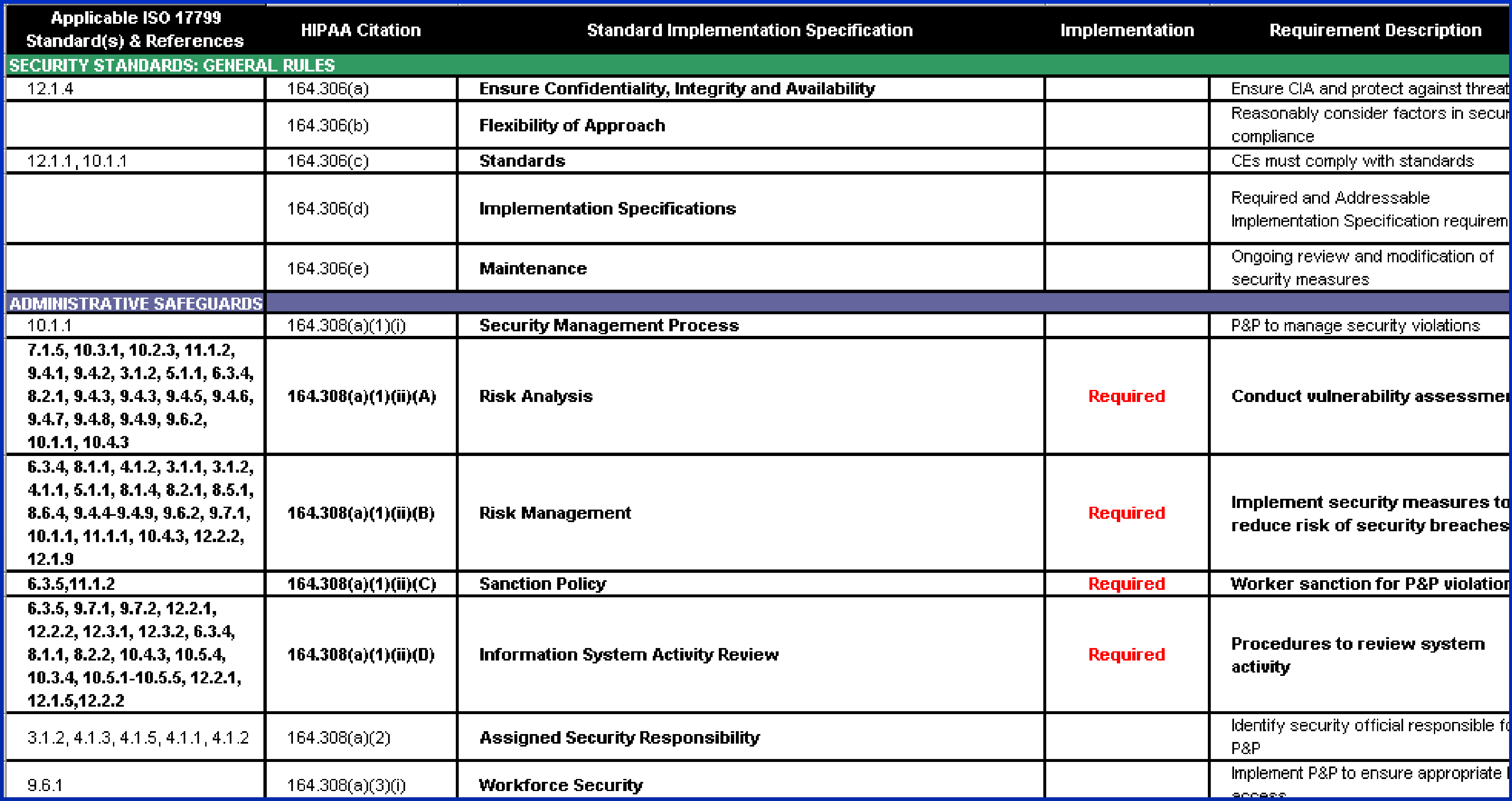
Division of Mental Health, Developmental Disabilities and Substance Abuse Services
North Carolina

Responsibility Matrix



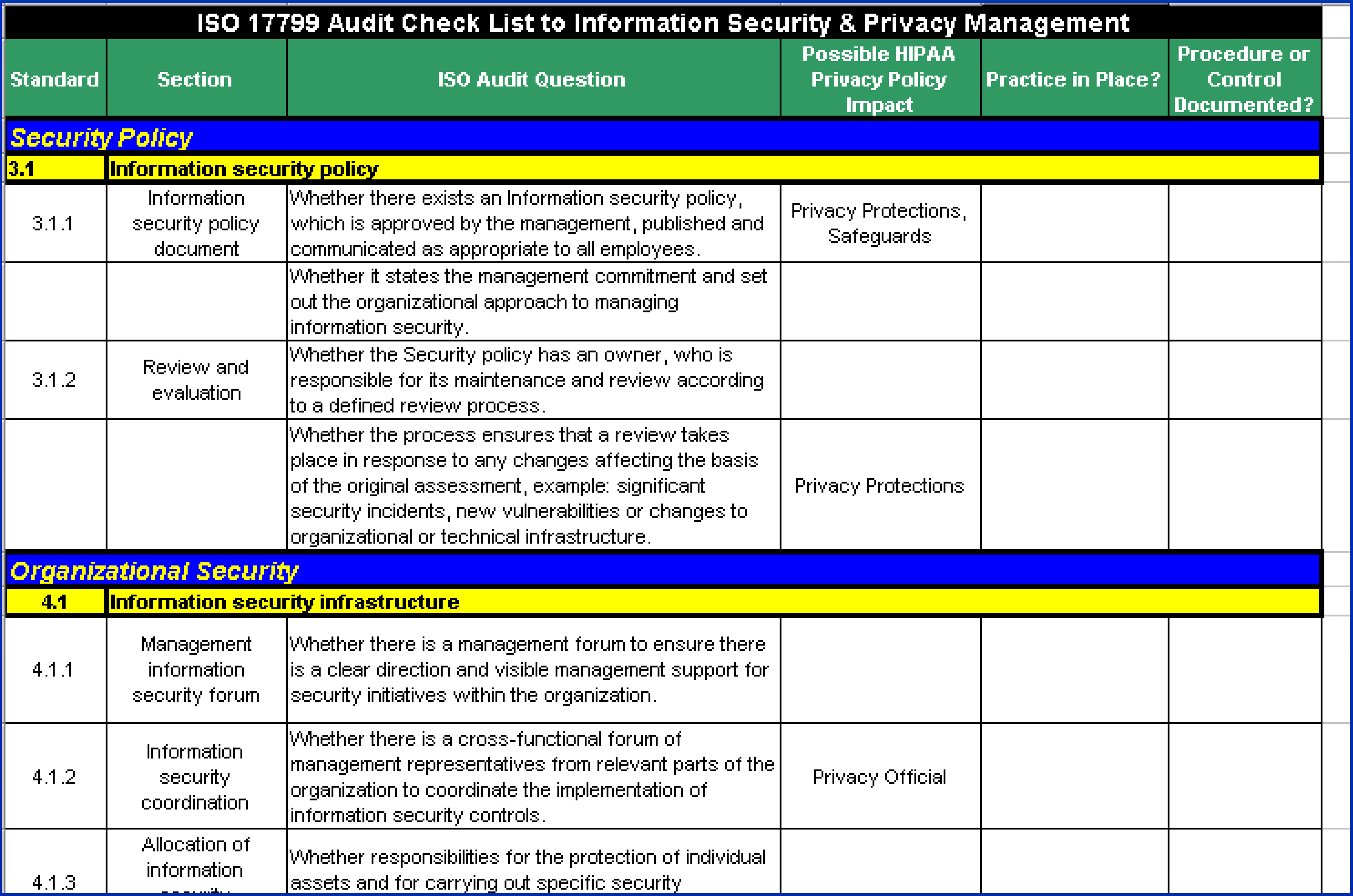
HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Privacy Officer	Compliance Office	Security Officer	IT Managers	Network or System Administrator	DB Administrator	D
164.306(a)	**Ensure Confidentiality, Integrity and Availability**							
164.306(b)	**Flexibility of Approach**							
164.306(c)	**Standards**							
164.306(d)	**Implementation Specifications**							
164.306(e)	**Maintenance**							
ADMINISTRATIVE SAFEGUARDS								
164.308(a)(1)(i)	**Security Management Process**	Awareness	Notification	Policy	Procedures	Procedures	Procedures	
164.308(a)(1)(ii)(A)	Risk Analysis	Awareness	Notification	Oversee	Assessment	Assessment		
164.308(a)(1)(ii)(B)	Risk Management	Awareness	Notification	Policy	Procedures	Measures		
164.308(a)(1)(ii)(C)	Sanction Policy		Records	Policy	Management			
164.308(a)(1)(ii)(D)	Information System Activity Review			Event Rept.	Event Rept.	Sys Auditing		
164.308(a)(2)	**Assigned Security Responsibility**			Authority				
164.308(a)(3)(i)	**Workforce Security**			Policy	Manage			
164.308(a)(3)(ii)(A)	Authorization and/or Supervision			Policy	Authorize	Supervise		
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure			Policy	Clearance			
164.308(a)(3)(ii)(C)	Termination Procedures		Policy		Manage			
164.308(a)(4)(i)	**Information Access Management**	Awareness	Job Desp	Awareness	Awareness			
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions							
164.308(a)(4)(ii)(B)	Access Authorization							
164.308(a)(4)(ii)(C)	Access Establishment and Modification				Change Form			
164.308(a)(5)(i)	**Security Awareness Training**							
164.308(a)(5)(ii)(A)	Security Reminders							
164.308(a)(5)(ii)(B)	Protection from Malicious Software							
164.308(a)(5)(ii)(C)	Log-in Monitoring							
164.308(a)(5)(ii)(D)	Password Management							
164.308(a)(6)(i)	**Security Incident Procedures**							
164.308(a)(6)(ii)	Response and Reporting			Incident Rep.	Incident Rep.	Monitor		
164.308(a)(7)(i)	**Contingency Plan**				BCP	Recovery	Recovery	

ISO Crosswalk



Applicable ISO 17799 Standard(s) & References	HIPAA Citation	Standard Implementation Specification	Implementation	Requirement Description
SECURITY STANDARDS: GENERAL RULES				
12.1.4	164.306(a)	**Ensure Confidentiality, Integrity and Availability**		Ensure CIA and protect against threat
	164.306(b)	**Flexibility of Approach**		Reasonably consider factors in secur compliance
12.1.1, 10.1.1	164.306(c)	**Standards**		CEs must comply with standards
	164.306(d)	**Implementation Specifications**		Required and Addressable Implementation Specification requirem
	164.306(e)	**Maintenance**		Ongoing review and modification of security measures
ADMINISTRATIVE SAFEGUARDS				
10.1.1	164.308(a)(1)(i)	**Security Management Process**		P&P to manage security violations
7.1.5, 10.3.1, 10.2.3, 11.1.2, 9.4.1, 9.4.2, 3.1.2, 5.1.1, 6.3.4, 8.2.1, 9.4.3, 9.4.3, 9.4.5, 9.4.6, 9.4.7, 9.4.8, 9.4.9, 9.6.2, 10.1.1, 10.4.3	**164.308(a)(1)(ii)(A)**	**Risk Analysis**	**Required**	**Conduct vulnerability assessme**
6.3.4, 8.1.1, 4.1.2, 3.1.1, 3.1.2, 4.1.1, 5.1.1, 8.1.4, 8.2.1, 8.5.1, 8.6.4, 9.4.4-9.4.9, 9.6.2, 9.7.1, 10.1.1, 11.1.1, 10.4.3, 12.2.2, 12.1.9	**164.308(a)(1)(ii)(B)**	**Risk Management**	**Required**	**Implement security measures to reduce risk of security breaches**
6.3.5,11.1.2	**164.308(a)(1)(ii)(C)**	**Sanction Policy**	**Required**	**Worker sanction for P&P violation**
6.3.5, 9.7.1, 9.7.2, 12.2.1, 12.2.2, 12.3.1, 12.3.2, 6.3.4, 8.1.1, 8.2.2, 10.4.3, 10.5.4, 10.3.4, 10.5.1-10.5.5, 12.2.1, 12.1.5,12.2.2	**164.308(a)(1)(ii)(D)**	**Information System Activity Review**	**Required**	**Procedures to review system activity**
3.1.2, 4.1.3, 4.1.5, 4.1.1, 4.1.2	164.308(a)(2)	**Assigned Security Responsibility**		Identify security official responsible f P&P
9.6.1	164.308(a)(3)(i)	**Workforce Security**		Implement P&P to ensure appropriate access

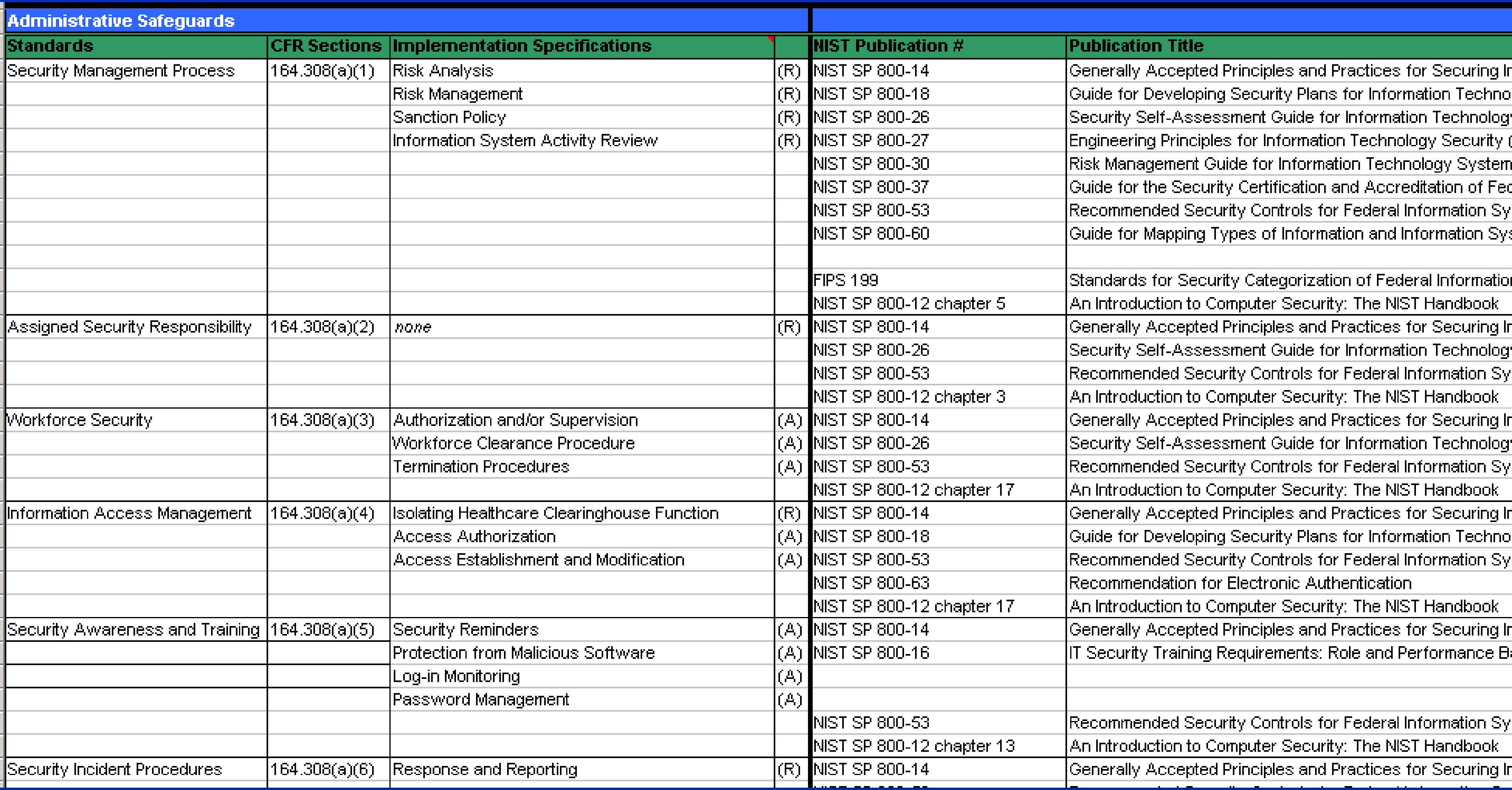
ISO 17799 Crosswalk



ISO 17799 Audit Check List to Information Security & Privacy Management

Standard	Section	ISO Audit Question	Possible HIPAA Privacy Policy Impact	Practice in Place?	Procedure or Control Documented?
Security Policy					
3.1	**Information security policy**				
3.1.1	Information security policy document	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.	Privacy Protections, Safeguards		
		Whether it states the management commitment and set out the organizational approach to managing information security.			
3.1.2	Review and evaluation	Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.			
		Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.	Privacy Protections		
Organizational Security					
4.1	**Information security infrastructure**				
4.1.1	Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization.			
4.1.2	Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	Privacy Official		
4.1.3	Allocation of information	Whether responsibilities for the protection of individual assets and for carrying out specific security			

NIST Crosswalk



Administrative Safeguards

Standards	CFR Sections	Implementation Specifications		NIST Publication #	Publication Title
Security Management Process	164.308(a)(1)	Risk Analysis	(R)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In
		Risk Management	(R)	NIST SP 800-18	Guide for Developing Security Plans for Information Techno
		Sanction Policy	(R)	NIST SP 800-26	Security Self-Assessment Guide for Information Technolog
		Information System Activity Review	(R)	NIST SP 800-27	Engineering Principles for Information Technology Security (
				NIST SP 800-30	Risk Management Guide for Information Technology System
				NIST SP 800-37	Guide for the Security Certification and Accreditation of Fed
				NIST SP 800-53	Recommended Security Controls for Federal Information Sy
				NIST SP 800-60	Guide for Mapping Types of Information and Information Sys
				FIPS 199	Standards for Security Categorization of Federal Informatio
				NIST SP 800-12 chapter 5	An Introduction to Computer Security: The NIST Handbook
Assigned Security Responsibility	164.308(a)(2)	*none*	(R)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In
				NIST SP 800-26	Security Self-Assessment Guide for Information Technolog
				NIST SP 800-53	Recommended Security Controls for Federal Information Sy
				NIST SP 800-12 chapter 3	An Introduction to Computer Security: The NIST Handbook
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In
		Workforce Clearance Procedure	(A)	NIST SP 800-26	Security Self-Assessment Guide for Information Technolog
		Termination Procedures	(A)	NIST SP 800-53	Recommended Security Controls for Federal Information Sy
				NIST SP 800-12 chapter 17	An Introduction to Computer Security: The NIST Handbook
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function	(R)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In
		Access Authorization	(A)	NIST SP 800-18	Guide for Developing Security Plans for Information Techno
		Access Establishment and Modification	(A)	NIST SP 800-53	Recommended Security Controls for Federal Information Sy
				NIST SP 800-63	Recommendation for Electronic Authentication
				NIST SP 800-12 chapter 17	An Introduction to Computer Security: The NIST Handbook
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In
		Protection from Malicious Software	(A)	NIST SP 800-16	IT Security Training Requirements: Role and Performance Ba
		Log-in Monitoring	(A)		
		Password Management	(A)		
				NIST SP 800-53	Recommended Security Controls for Federal Information Sy
				NIST SP 800-12 chapter 13	An Introduction to Computer Security: The NIST Handbook
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)	NIST SP 800-14	Generally Accepted Principles and Practices for Securing In

Self-assessment / Gap Analysis Tools Developed by NCHICA Member Volunteers

HIPAA EarlyView™ Security

Focus on your compliance plan with this powerful software tool

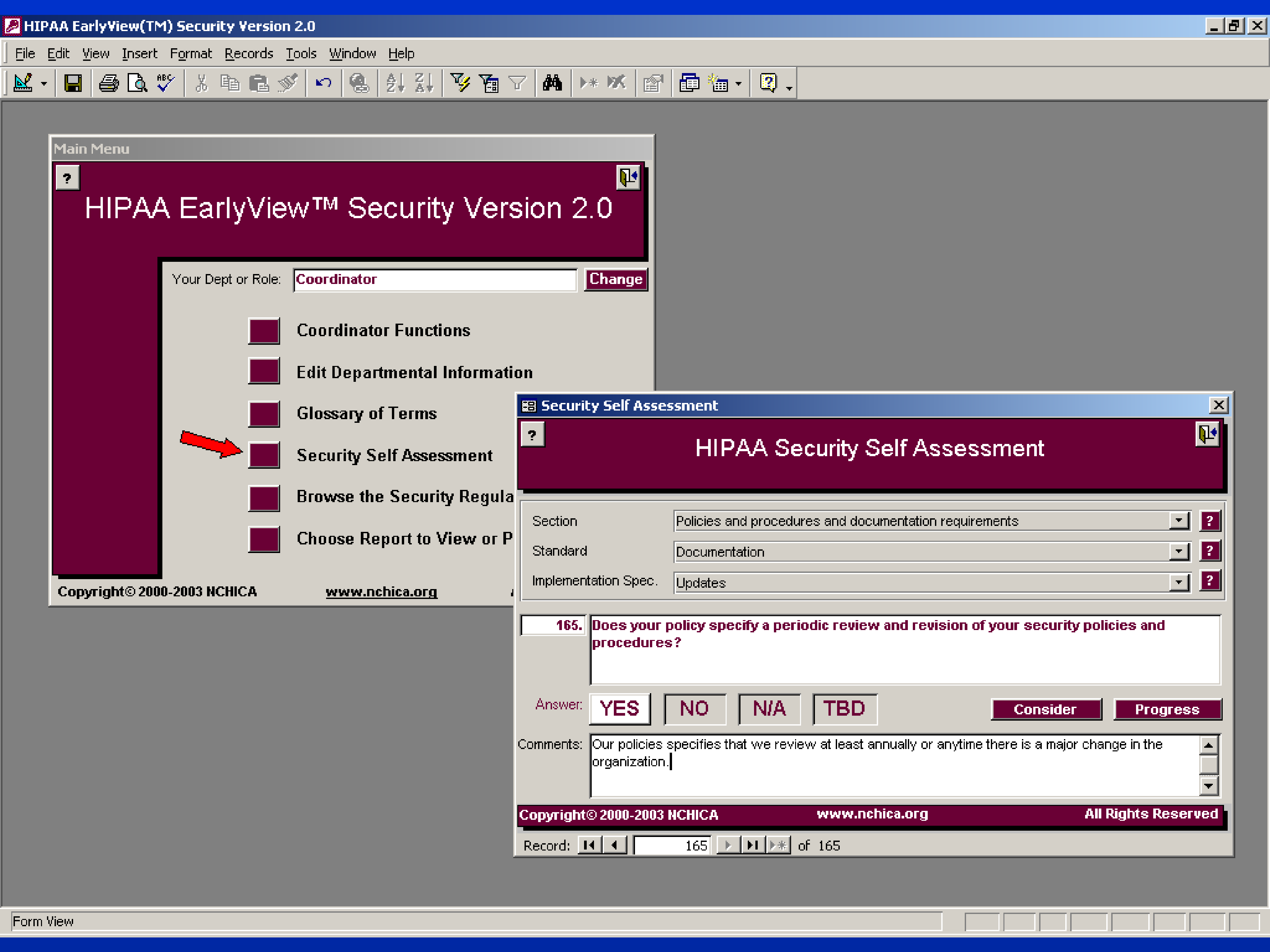
HIPAA EarlyView™ Privacy

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



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?

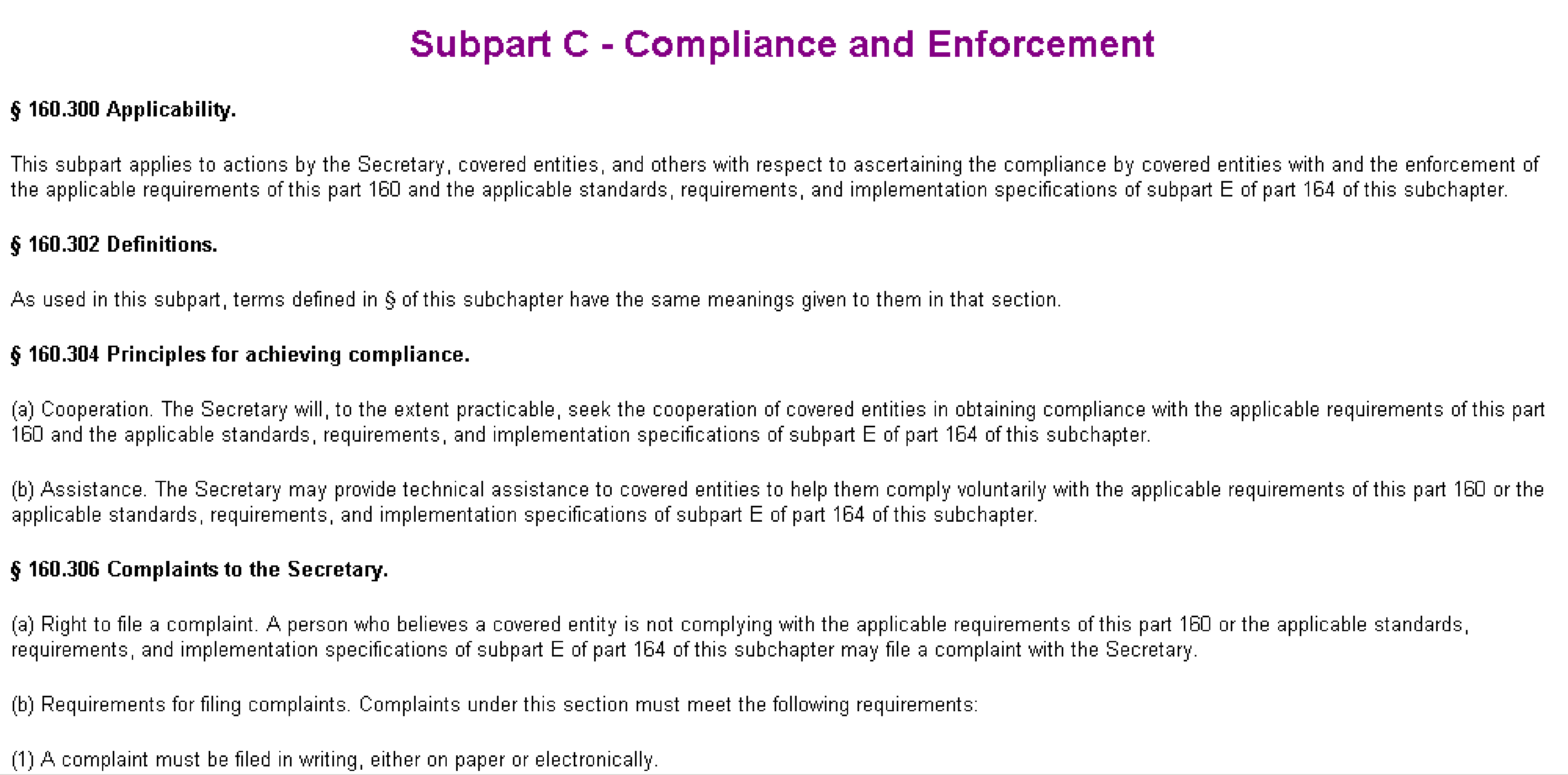
Answer:

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.

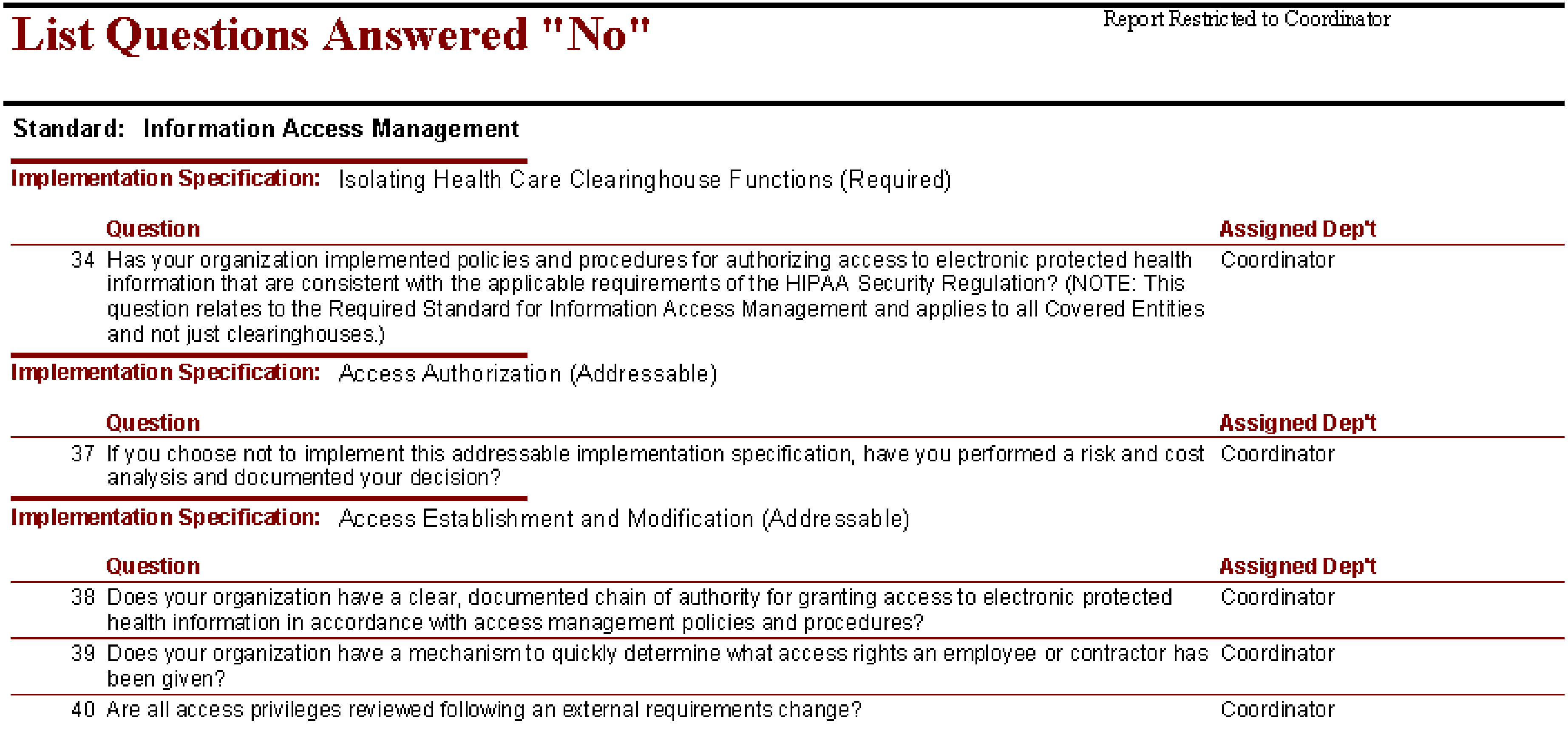
§ 160.306 Complaints to the Secretary.

(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 Answered "No"

Report Restricted to Coordinator

Standard: Information Access Management

Implementation Specification: Isolating Health Care Clearinghouse Functions (Required)

	Question	Assigned Dep't
34	Has your organization implemented policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the HIPAA Security Regulation? (NOTE: This question relates to the Required Standard for Information Access Management and applies to all Covered Entities and not just clearinghouses.)	Coordinator

Implementation Specification: Access Authorization (Addressable)

	Question	Assigned Dep't
37	If you choose not to implement this addressable implementation specification, have you performed a risk and cost analysis and documented your decision?	Coordinator

Implementation Specification: Access Establishment and Modification (Addressable)

	Question	Assigned Dep't
38	Does your organization have a clear, documented chain of authority for granting access to electronic protected health information in accordance with access management policies and procedures?	Coordinator
39	Does your organization have a mechanism to quickly determine what access rights an employee or contractor has been given?	Coordinator
40	Are all access privileges reviewed following an external requirements change?	Coordinator

HIPAA EarlyView™ Tools Extenders

DocASSURE	www.jasi.com
ParamoreConsultingInc.	www.paramoreconsulting.com
PARENTE RANDOLPH Accountants & Consultants	www.parentenet.com
ComplyAssistant	www.complyassistant.com

Coordination 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/

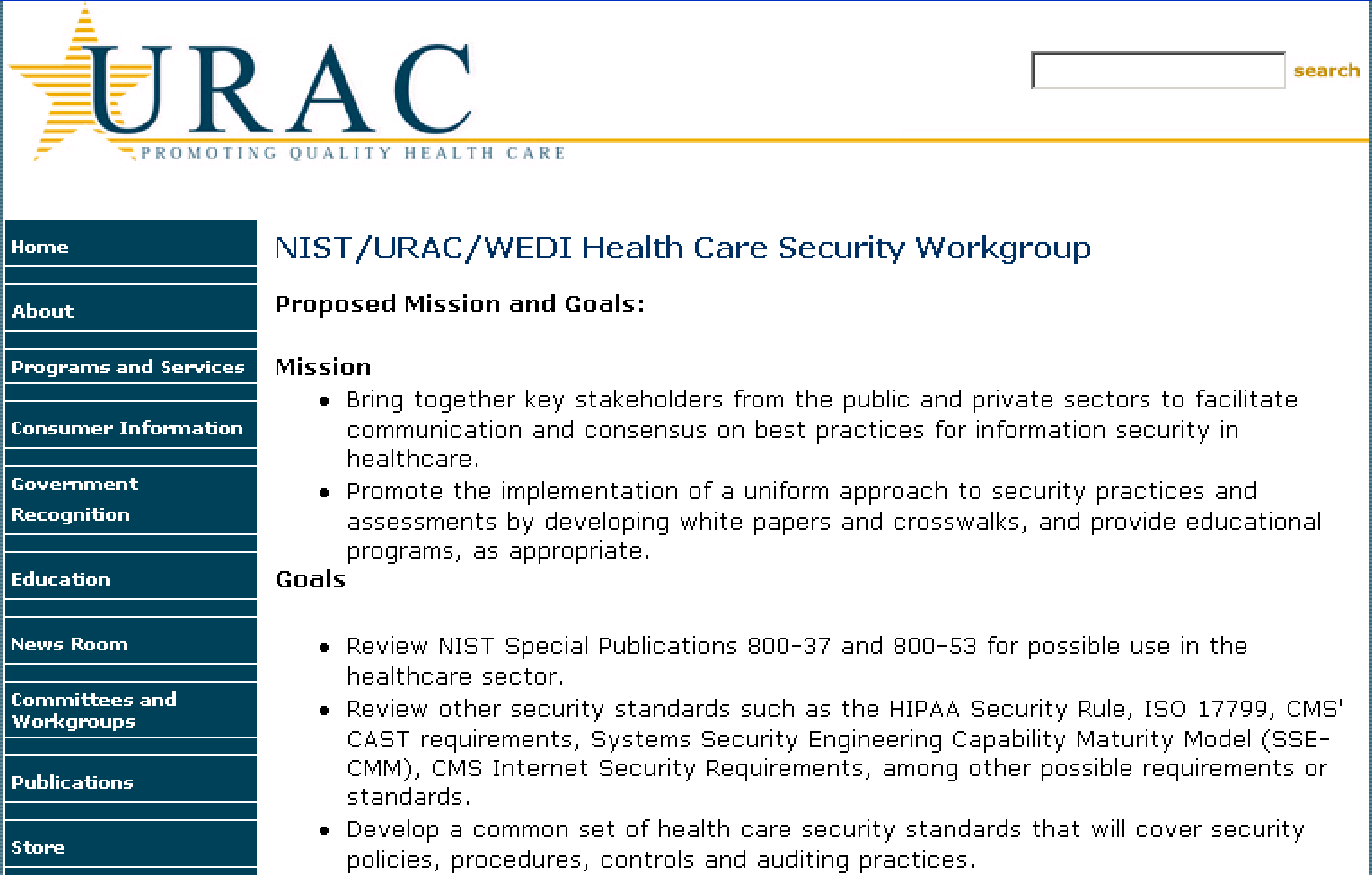
Other Standards to Consider (cont.)

- 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

Coordination w/ Other Regulations and Standards

- Numerous Crosswalks developed
- Borrow and adapt
- Add considerations for various state statutes, regulations and case law
- Collaborate on interpretation with peers in your area
- Potential activity within a Regional SNIP Affiliate organization (RSA)
- Integrate into your compliance plans

NIST/URAC/WEDI Health Care Security Workgroup



NIST/URAC/WEDI Health Care Security Workgroup

Proposed Mission and Goals:

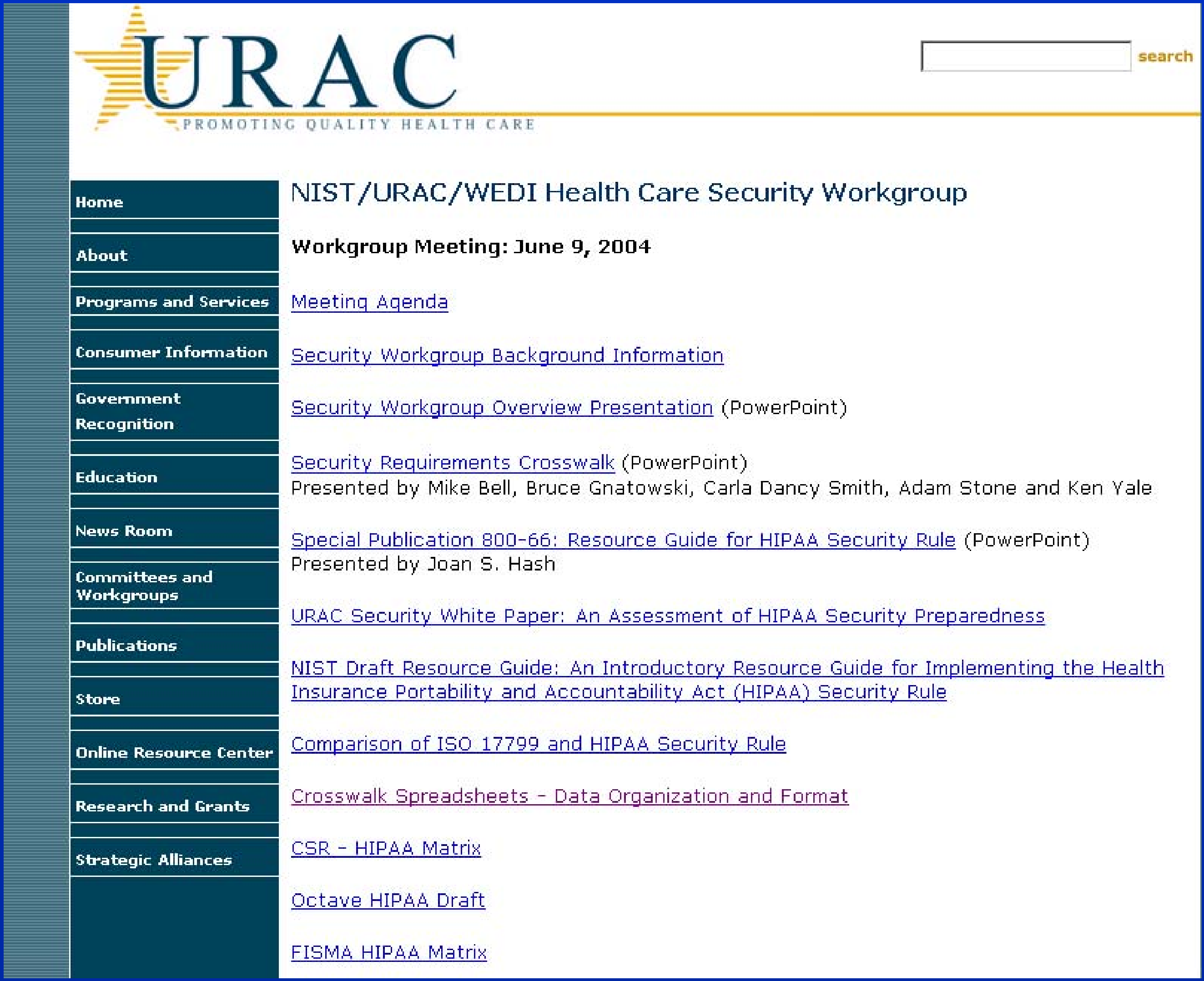
Mission

- Bring together key stakeholders from the public and private sectors to facilitate communication and consensus on best practices for information security in healthcare.
- Promote the implementation of a uniform approach to security practices and assessments by developing white papers and crosswalks, and provide educational programs, as appropriate.

Goals

- Review NIST Special Publications 800-37 and 800-53 for possible use in the healthcare sector.
- Review other security standards such as the HIPAA Security Rule, ISO 17799, CMS' CAST requirements, Systems Security Engineering Capability Maturity Model (SSE-CMM), CMS Internet Security Requirements, among other possible requirements or standards.
- Develop a common set of health care security standards that will cover security policies, procedures, controls and auditing practices.

NIST/URAC/WEDI Deliverables



NIST/URAC/WEDI Health Care Security Workgroup

Workgroup Meeting: June 9, 2004

Meeting Agenda

Security Workgroup Background Information

Security Workgroup Overview Presentation (PowerPoint)

Security Requirements Crosswalk (PowerPoint)
Presented by Mike Bell, Bruce Gnatowski, Carla Dancy Smith, Adam Stone and Ken Yale

Special Publication 800-66: Resource Guide for HIPAA Security Rule (PowerPoint)
Presented by Joan S. Hash

URAC Security White Paper: An Assessment of HIPAA Security Preparedness

NIST Draft Resource Guide: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Comparison of ISO 17799 and HIPAA Security Rule

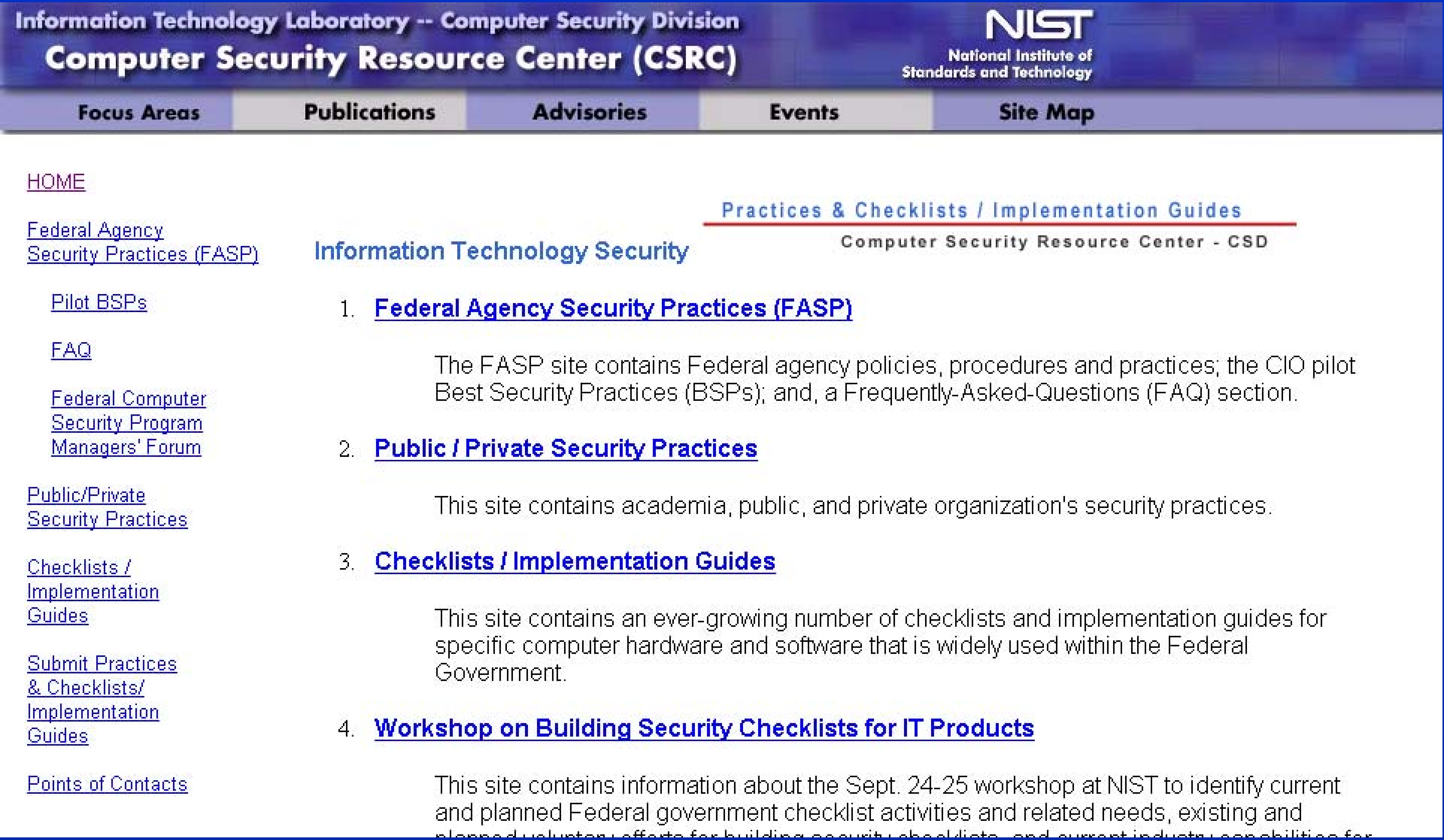
Crosswalk Spreadsheets - Data Organization and Format

CSR - HIPAA Matrix

Octave HIPAA Draft

FISMA HIPAA Matrix

NIST


Information Technology Laboratory -- Computer Security Division
Computer Security Resource Center (CSRC)
NIST
National Institute of Standards and Technology
Focus Areas
Publications
Advisories
Events
Site Map
HOME
Federal Agency Security Practices (FASP)
Pilot BSPs
FAQ
Federal Computer Security Program Managers' Forum
Public/Private Security Practices
Checklists / Implementation Guides
Submit Practices & Checklists/ Implementation Guides
Points of Contacts

Practices & Checklists / Implementation Guides

Computer Security Resource Center - CSD

Information Technology Security

1. **Federal Agency Security Practices (FASP)**

   The FASP site contains Federal agency policies, procedures and practices; the CIO pilot Best Security Practices (BSPs); and, a Frequently-Asked-Questions (FAQ) section.

2. **Public / Private Security Practices**

   This site contains academia, public, and private organization's security practices.

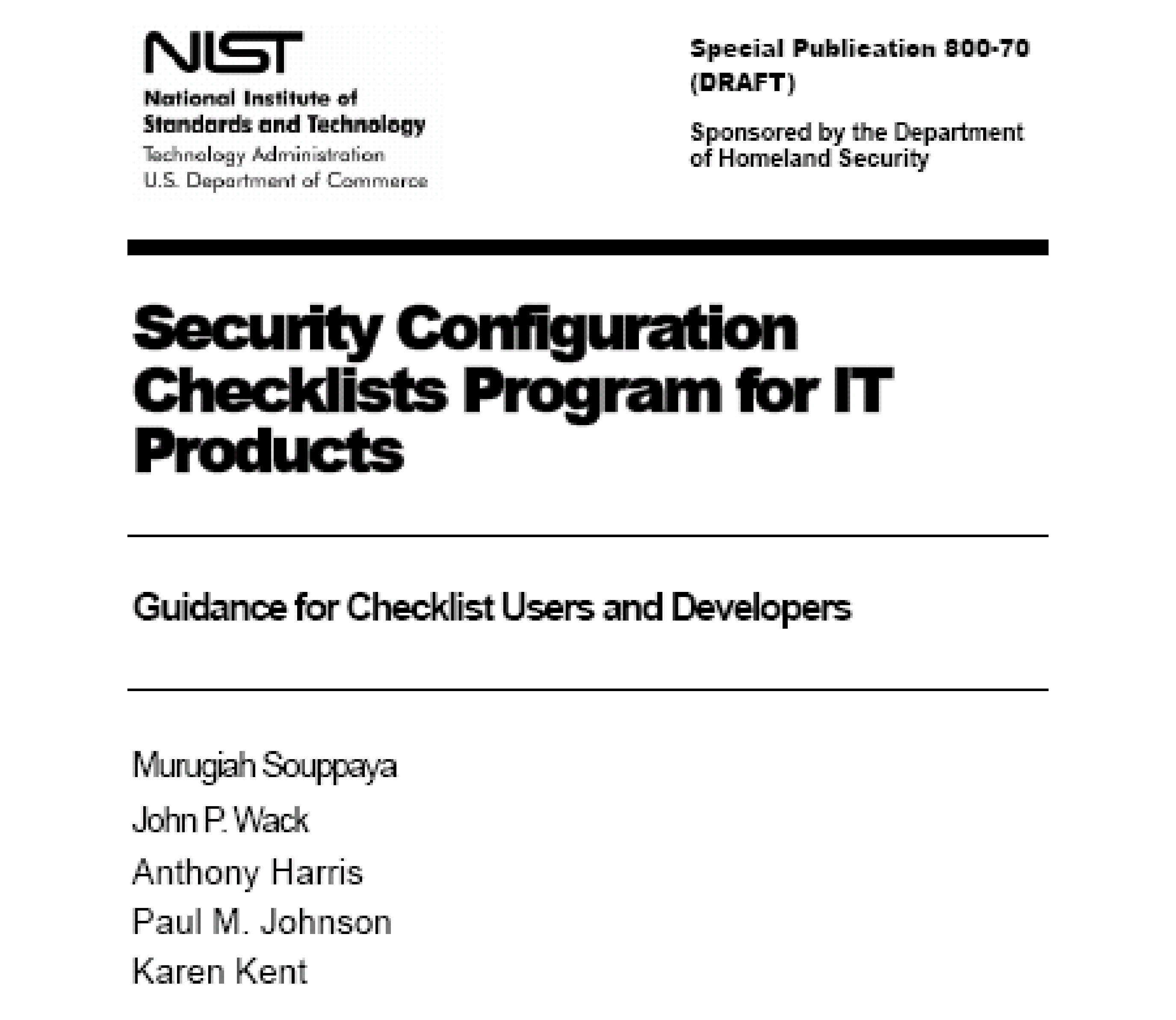
3. **Checklists / Implementation Guides**

   This site contains an ever-growing number of checklists and implementation guides for specific computer hardware and software that is widely used within the Federal Government.

4. **Workshop on Building Security Checklists for IT Products**

   This site contains information about the Sept. 24-25 workshop at NIST to identify current and planned Federal government checklist activities and related needs, existing and planned voluntary efforts for building security checklists, and current industry capabilities for

NIST



NIST

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-70 (DRAFT)

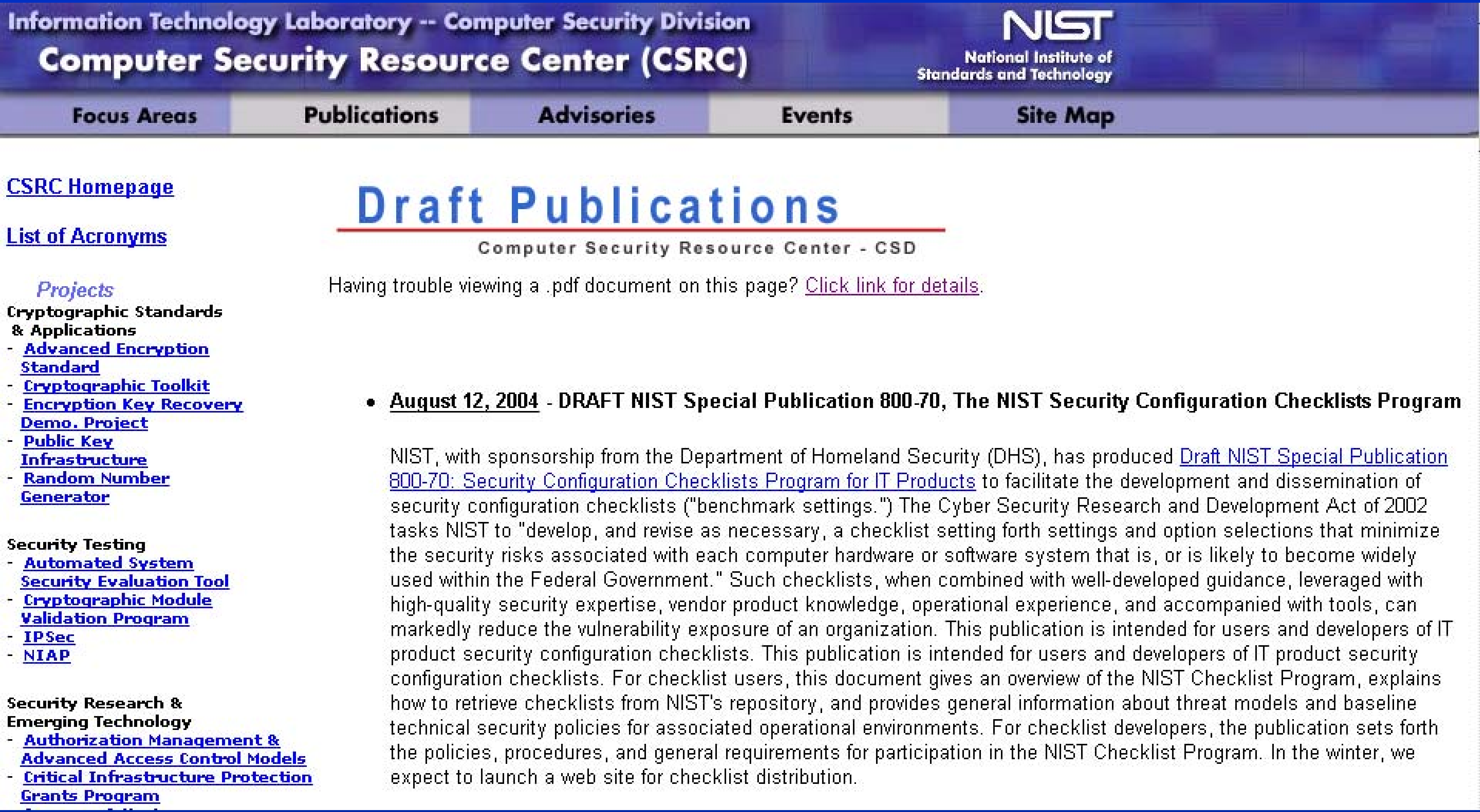
Sponsored by the Department of Homeland Security

Security Configuration Checklists Program for IT Products

Guidance for Checklist Users and Developers

Murugiah Souppaya
John P. Wack
Anthony Harris
Paul M. Johnson
Karen Kent

NIST 800-70 Checklist Program


Information Technology Laboratory -- Computer Security Division
Computer Security Resource Center (CSRC)
NIST
National Institute of Standards and Technology
Focus Areas
Publications
Advisories
Events
Site Map
CSRC Homepage
List of Acronyms
Projects
Cryptographic Standards & Applications
- Advanced Encryption Standard
- Cryptographic Toolkit
- Encryption Key Recovery Demo. Project
- Public Key Infrastructure
- Random Number Generator
Security Testing
- Automated System Security Evaluation Tool
- Cryptographic Module Validation Program
- IPSec
- NIAP
Security Research & Emerging Technology
- Authorization Management & Advanced Access Control Models
- Critical Infrastructure Protection Grants Program

Draft Publications

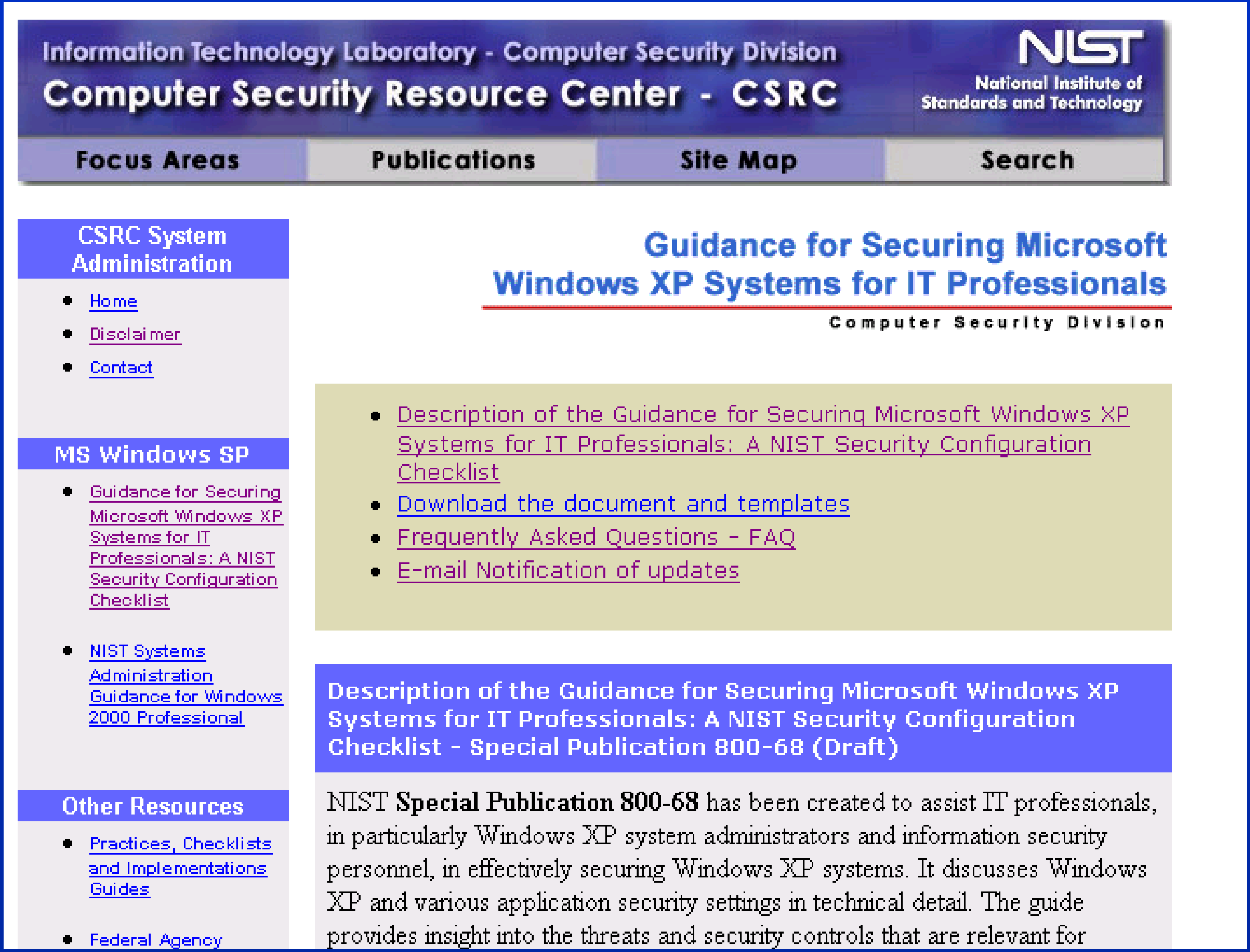
Computer Security Resource Center - CSD

Having trouble viewing a .pdf document on this page? Click link for details.

- August 12, 2004 - DRAFT NIST Special Publication 800-70, The NIST Security Configuration Checklists Program

  NIST, with sponsorship from the Department of Homeland Security (DHS), has produced Draft NIST Special Publication 800-70: Security Configuration Checklists Program for IT Products to facilitate the development and dissemination of security configuration checklists ("benchmark settings.") The Cyber Security Research and Development Act of 2002 tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government." Such checklists, when combined with well-developed guidance, leveraged with high-quality security expertise, vendor product knowledge, operational experience, and accompanied with tools, can markedly reduce the vulnerability exposure of an organization. This publication is intended for users and developers of IT product security configuration checklists. This publication is intended for users and developers of IT product security configuration checklists. For checklist users, this document gives an overview of the NIST Checklist Program, explains how to retrieve checklists from NIST's repository, and provides general information about threat models and baseline technical security policies for associated operational environments. For checklist developers, the publication sets forth the policies, procedures, and general requirements for participation in the NIST Checklist Program. In the winter, we expect to launch a web site for checklist distribution.

NIST XP Systems Guidance


Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC
NIST
National Institute of Standards and Technology
Focus Areas
Publications
Site Map
Search

CSRC System Administration

- Home
- Disclaimer
- Contact

MS Windows SP

- Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
- NIST Systems Administration Guidance for Windows 2000 Professional

Other Resources

- Practices, Checklists and Implementations Guides
- Federal Agency

Guidance for Securing Microsoft Windows XP Systems for IT Professionals

Computer Security Division

- Description of the Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
- Download the document and templates
- Frequently Asked Questions - FAQ
- E-mail Notification of updates

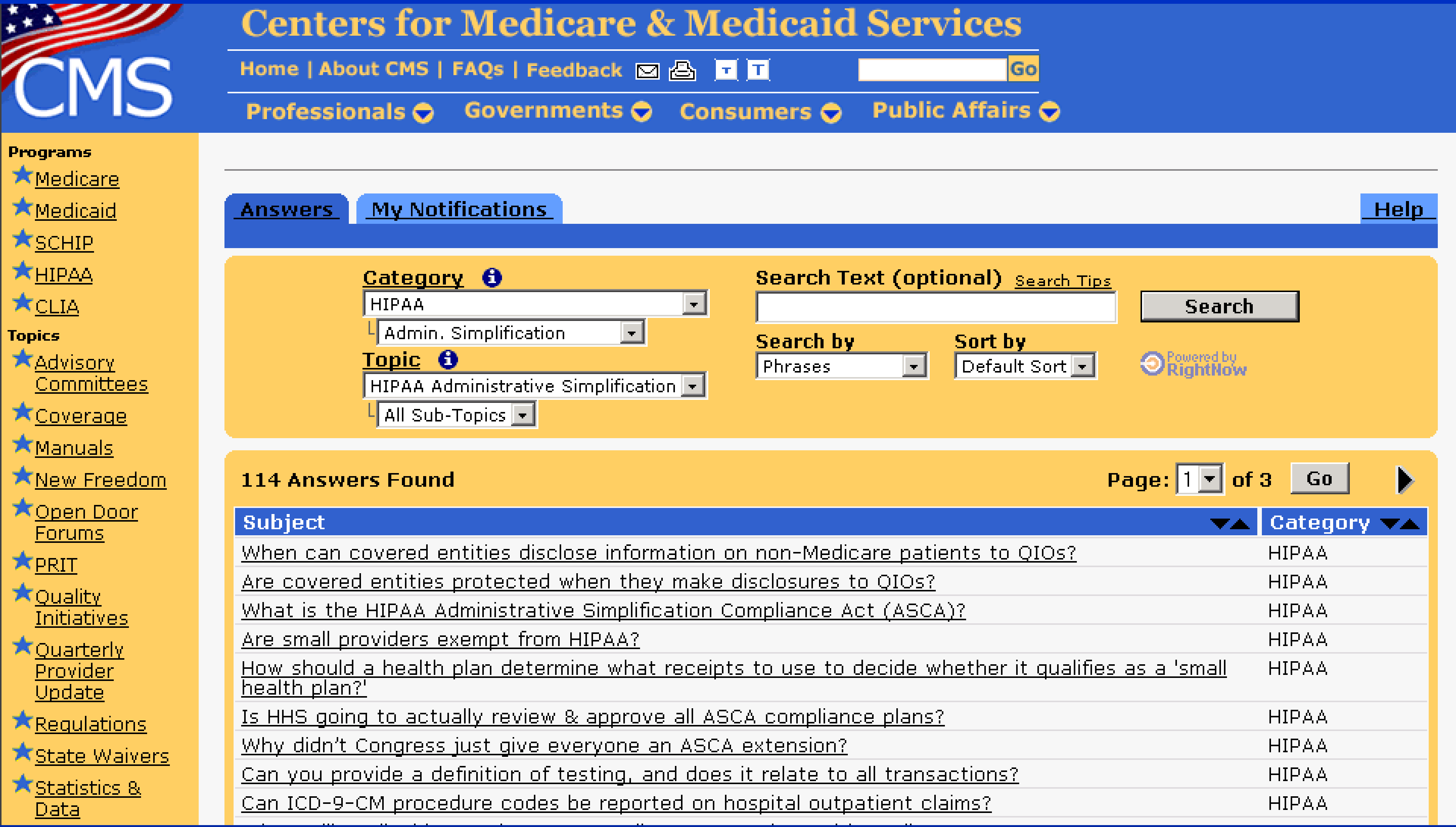
Description of the Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - Special Publication 800-68 (Draft)

NIST **Special Publication 800-68** has been created to assist IT professionals, in particularly Windows XP system administrators and information security personnel, in effectively securing Windows XP systems. It discusses Windows XP and various application security settings in technical detail. The guide provides insight into the threats and security controls that are relevant for

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
- csrc.nist.gov/itsec/
  - NIST site with crosswalks, policies, guidelines

CMS FAQs



Centers for Medicare & Medicaid Services

Programs

- Medicare
- Medicaid
- SCHIP
- HIPAA
- CLIA

Topics

- Advisory Committees
- Coverage
- Manuals
- New Freedom
- Open Door Forums
- PRIT
- Quality Initiatives
- Quarterly Provider Update
- Regulations
- State Waivers
- Statistics & Data

Category: HIPAA
└ Admin. Simplification

Topic: HIPAA Administrative Simplification
└ All Sub-Topics

Search Text (optional) Search Tips

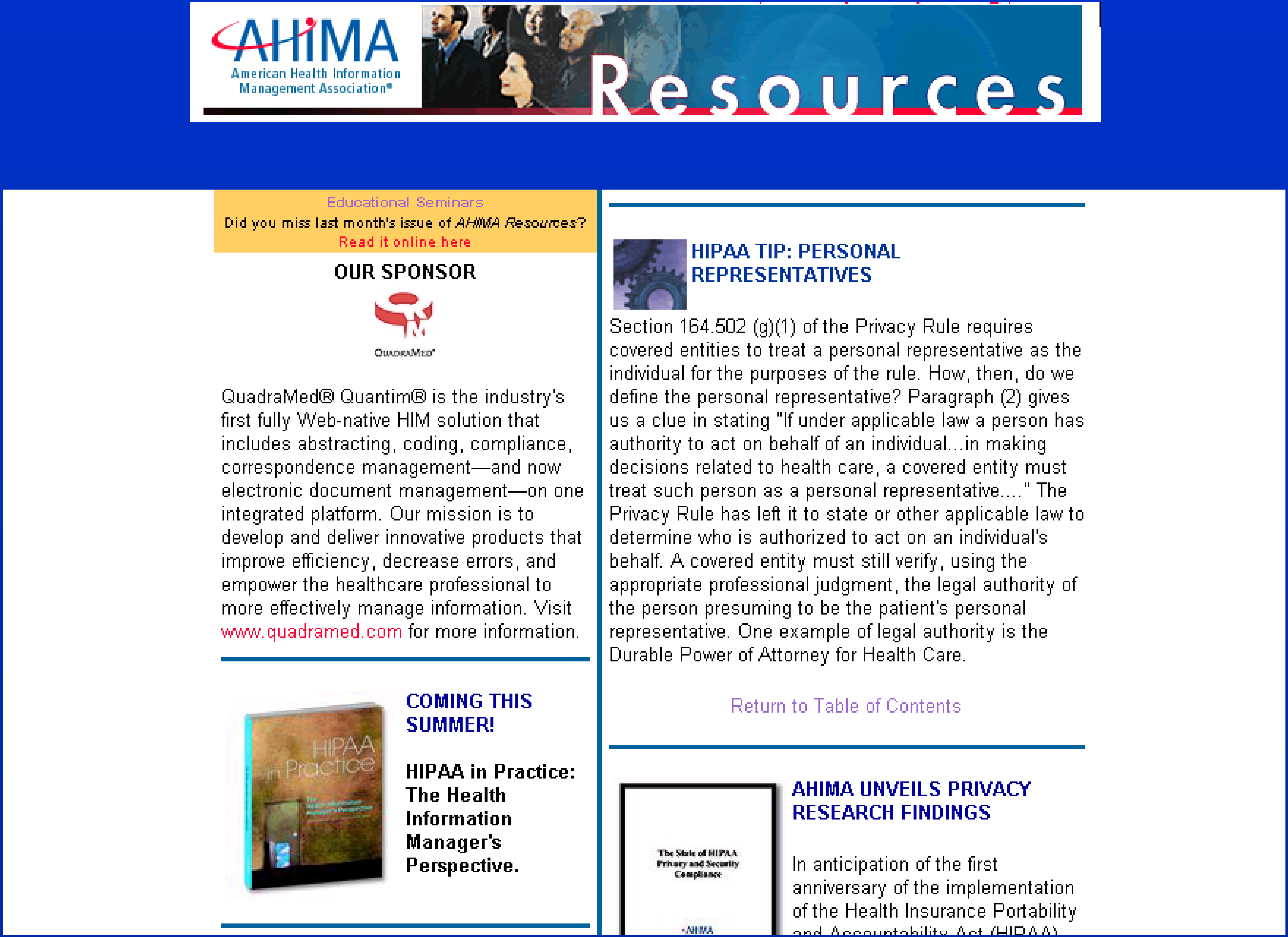
Search by: Phrases

Sort by: Default Sort

114 Answers Found

Page: 1 of 3 Go

Subject	Category
When can covered entities disclose information on non-Medicare patients to QIOs?	HIPAA
Are covered entities protected when they make disclosures to QIOs?	HIPAA
What is the HIPAA Administrative Simplification Compliance Act (ASCA)?	HIPAA
Are small providers exempt from HIPAA?	HIPAA
How should a health plan determine what receipts to use to decide whether it qualifies as a 'small health plan?'	HIPAA
Is HHS going to actually review & approve all ASCA compliance plans?	HIPAA
Why didn't Congress just give everyone an ASCA extension?	HIPAA
Can you provide a definition of testing, and does it relate to all transactions?	HIPAA
Can ICD-9-CM procedure codes be reported on hospital outpatient claims?	HIPAA


AHIMA
American Health Information Management Association®
Resources
QuadraMed®
HIPAA in Practice
The State of HIPAA Privacy and Security Compliance
AHIMA

Educational Seminars

Did you miss last month's issue of *AHIMA Resources*?

Read it online here

OUR SPONSOR

QuadraMed® Quantim® is the industry's first fully Web-native HIM solution that includes abstracting, coding, compliance, correspondence management—and now electronic document management—on one integrated platform. Our mission is to develop and deliver innovative products that improve efficiency, decrease errors, and empower the healthcare professional to more effectively manage information. Visit www.quadramed.com for more information.

COMING THIS SUMMER!

HIPAA in Practice: The Health Information Manager's Perspective.

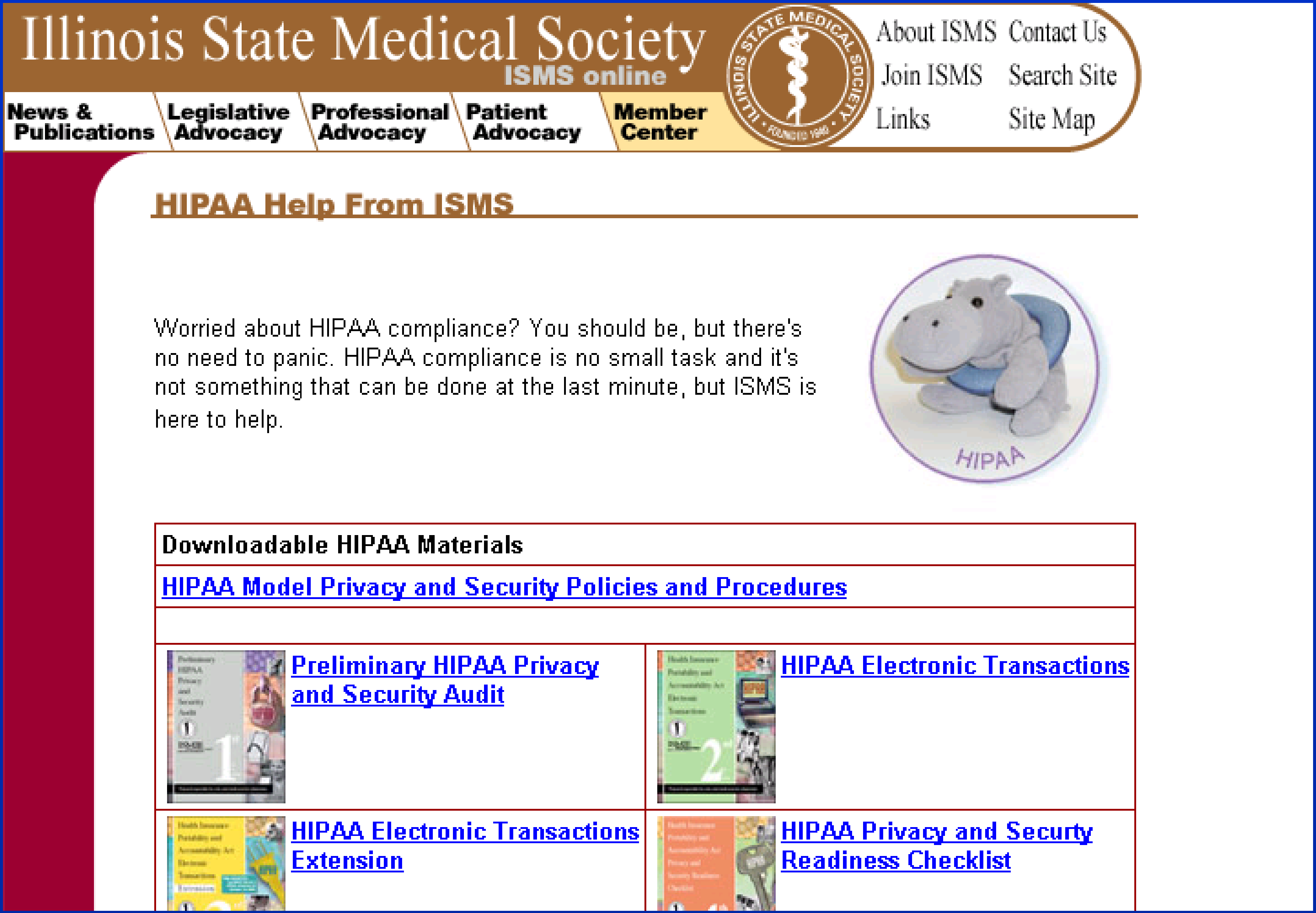
HIPAA TIP: PERSONAL REPRESENTATIVES

Section 164.502 (g)(1) of the Privacy Rule requires covered entities to treat a personal representative as the individual for the purposes of the rule. How, then, do we define the personal representative? Paragraph (2) gives us a clue in stating "If under applicable law a person has authority to act on behalf of an individual...in making decisions related to health care, a covered entity must treat such person as a personal representative...." The Privacy Rule has left it to state or other applicable law to determine who is authorized to act on an individual's behalf. A covered entity must still verify, using the appropriate professional judgment, the legal authority of the person presuming to be the patient's personal representative. One example of legal authority is the Durable Power of Attorney for Health Care.

Return to Table of Contents

AHIMA UNVEILS PRIVACY RESEARCH FINDINGS

In anticipation of the first anniversary of the implementation of the Health Insurance Portability and Accountability Act (HIPAA)

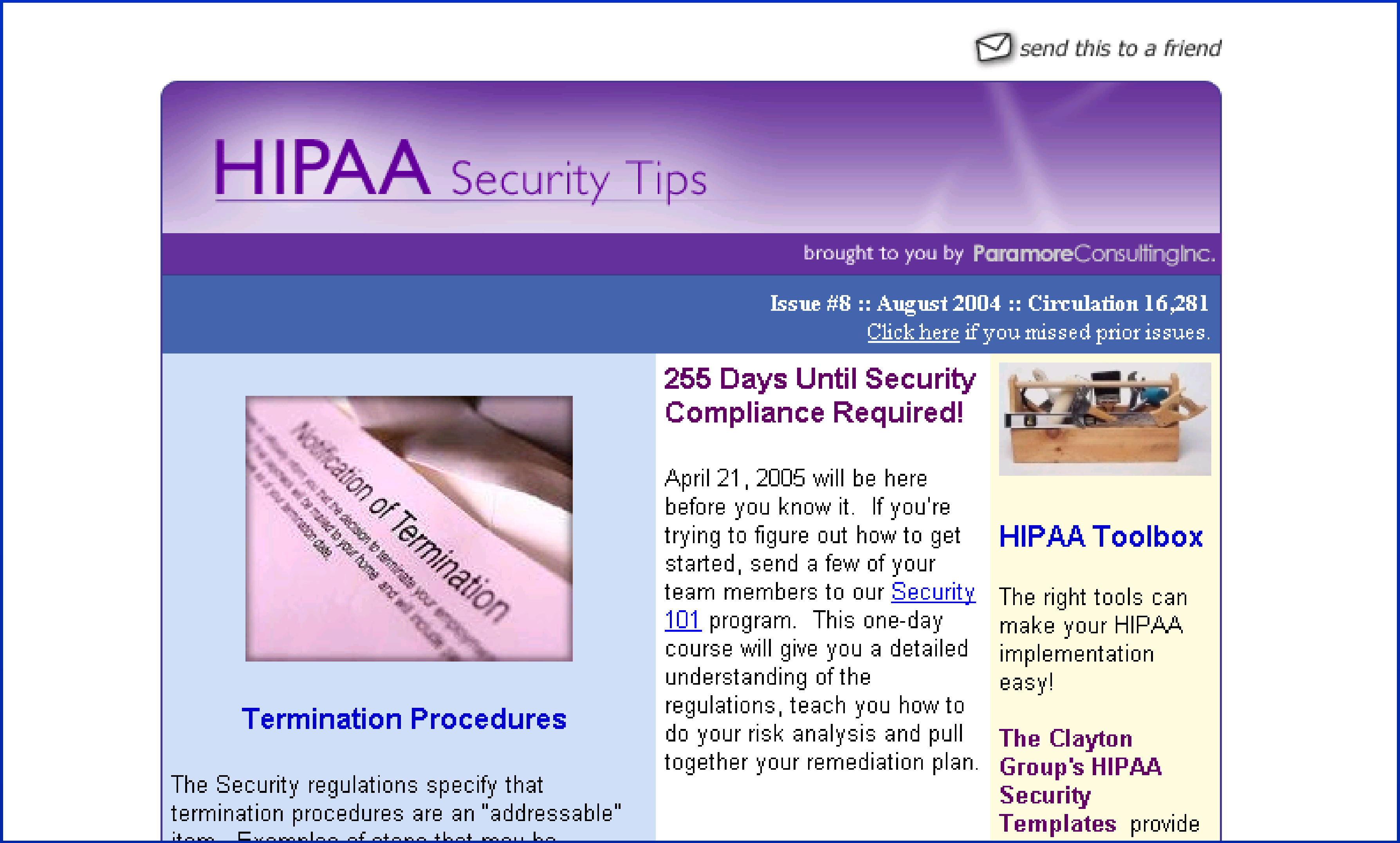


HIPAA Help From ISMS

Worried about HIPAA compliance? You should be, but there's no need to panic. HIPAA compliance is no small task and it's not something that can be done at the last minute, but ISMS is here to help.

Downloadable HIPAA Materials	
HIPAA Model Privacy and Security Policies and Procedures	
Preliminary HIPAA Privacy and Security Audit	HIPAA Electronic Transactions
HIPAA Electronic Transactions Extension	HIPAA Privacy and Securty Readiness Checklist

Free Newsletters



send this to a friend

HIPAA Security Tips

brought to you by ParamoreConsultingInc.

Issue #8 :: August 2004 :: Circulation 16,281
Click here if you missed prior issues.

Termination Procedures

The Security regulations specify that termination procedures are an "addressable" item. Examples of steps that may be

255 Days Until Security Compliance Required!

April 21, 2005 will be here before you know it. If you're trying to figure out how to get started, send a few of your team members to our Security 101 program. This one-day course will give you a detailed understanding of the regulations, teach you how to do your risk analysis and pull together your remediation plan.

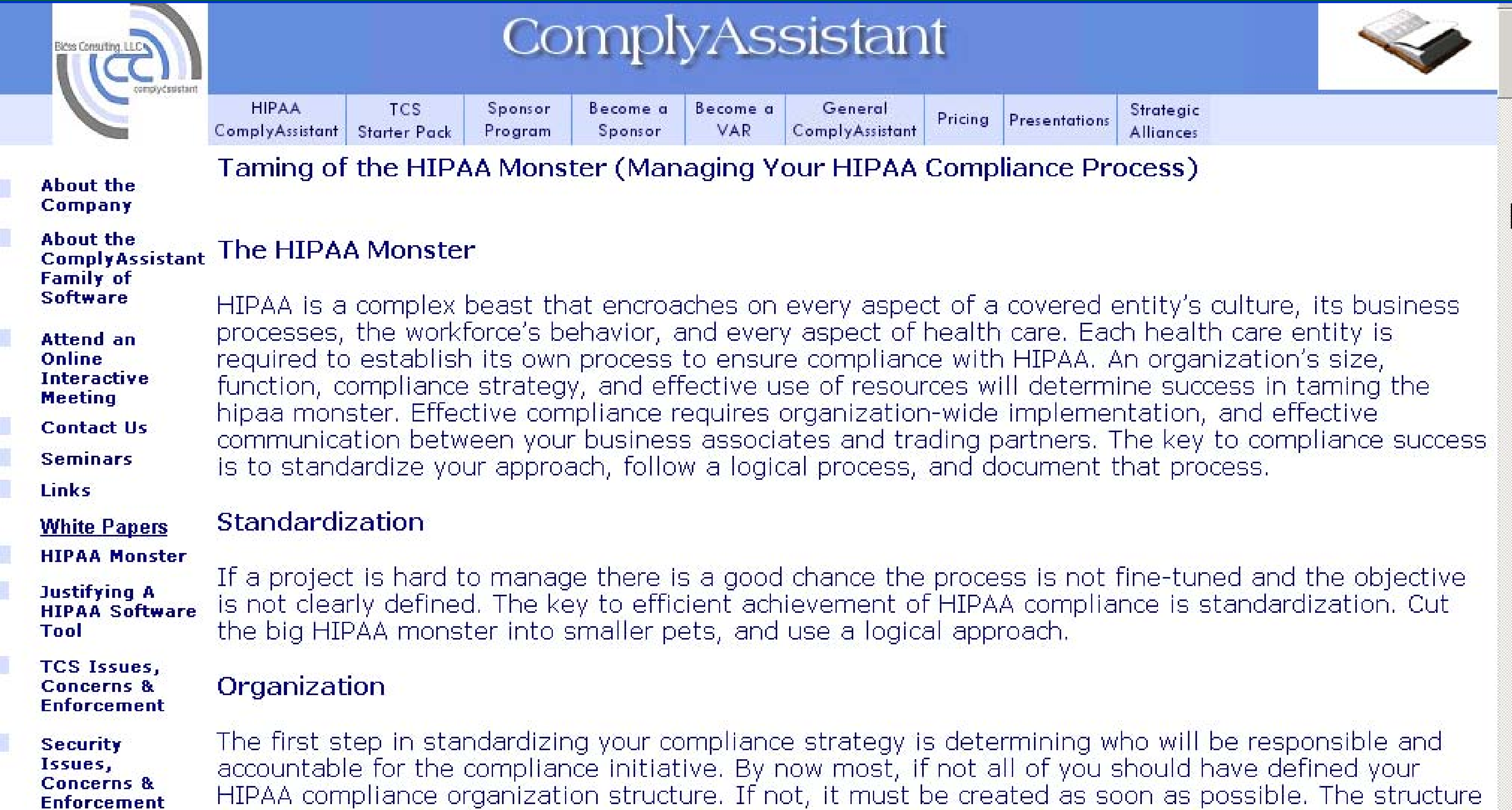
HIPAA Toolbox

The right tools can make your HIPAA implementation easy!

The Clayton Group's HIPAA Security Templates provide

www.paramoreconsulting.com

Getting Started White Paper



Taming of the HIPAA Monster (Managing Your HIPAA Compliance Process)

The HIPAA Monster

HIPAA is a complex beast that encroaches on every aspect of a covered entity's culture, its business processes, the workforce's behavior, and every aspect of health care. Each health care entity is required to establish its own process to ensure compliance with HIPAA. An organization's size, function, compliance strategy, and effective use of resources will determine success in taming the hipaa monster. Effective compliance requires organization-wide implementation, and effective communication between your business associates and trading partners. The key to compliance success is to standardize your approach, follow a logical process, and document that process.

Standardization

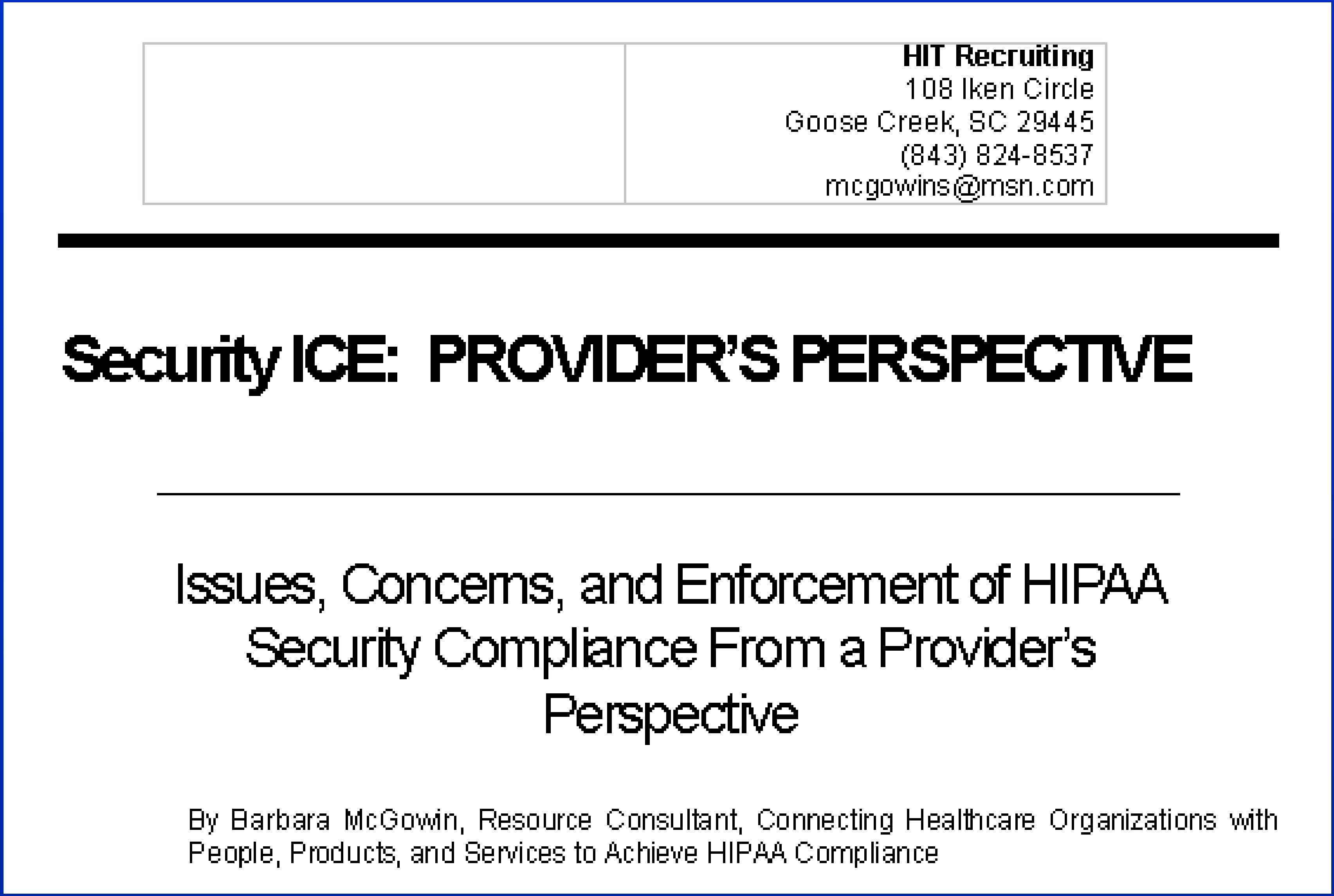
If a project is hard to manage there is a good chance the process is not fine-tuned and the objective is not clearly defined. The key to efficient achievement of HIPAA compliance is standardization. Cut the big HIPAA monster into smaller pets, and use a logical approach.

Organization

The first step in standardizing your compliance strategy is determining who will be responsible and accountable for the compliance initiative. By now most, if not all of you should have defined your HIPAA compliance organization structure. If not, it must be created as soon as possible. The structure

www.complyassistant.com

Overview White Paper



HIT Recruiting
108 Iken Circle
Goose Creek, SC 29445
(843) 824-8537
mcgowins@msn.com

Security ICE: PROVIDER'S PERSPECTIVE

Issues, Concerns, and Enforcement of HIPAA Security Compliance From a Provider's Perspective

By Barbara McGowin, Resource Consultant, Connecting Healthcare Organizations with People, Products, and Services to Achieve HIPAA Compliance

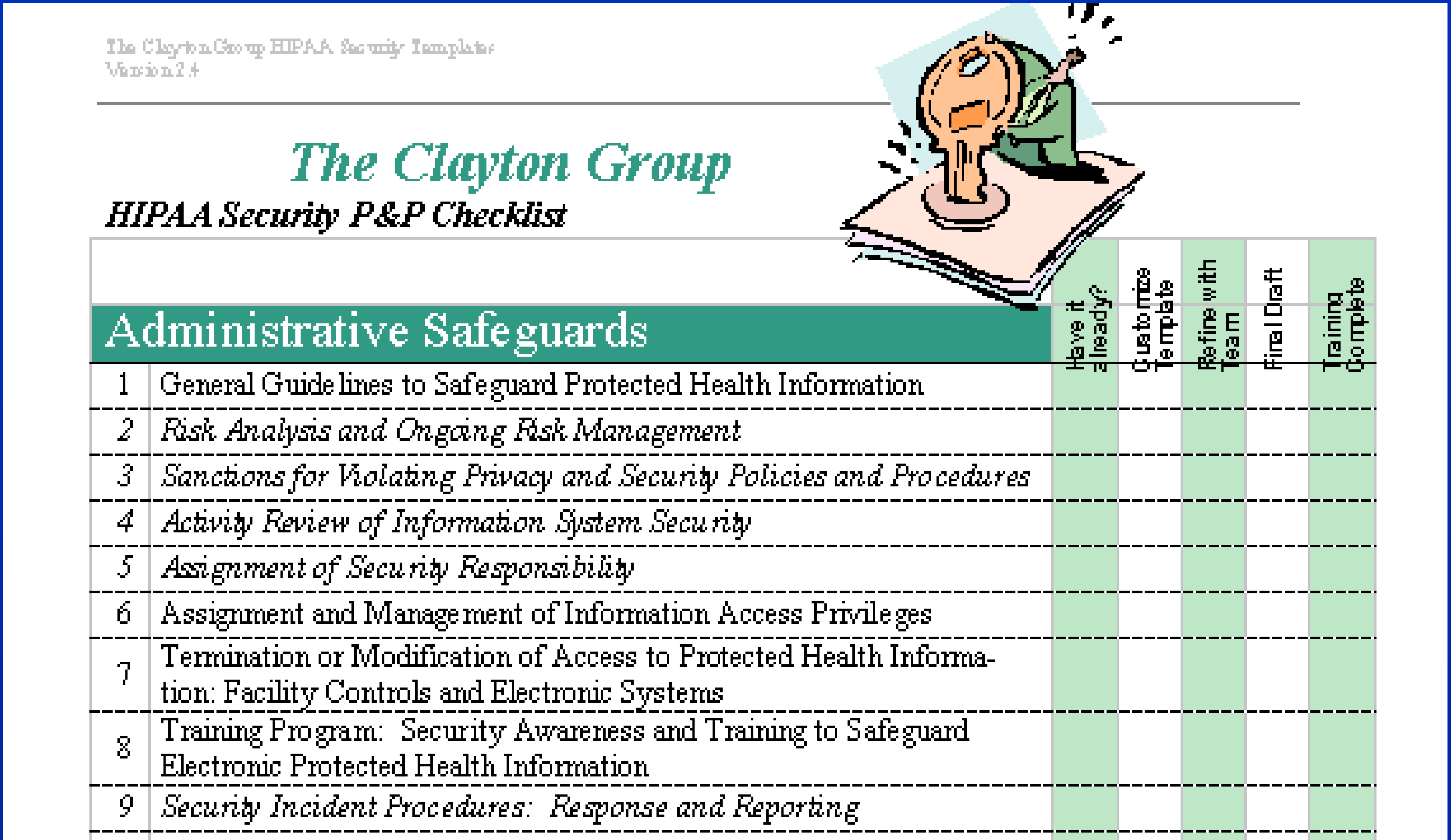
Policies & Procedures Checklist

The Clayton Group LLC

Healthcare Management Services

Suite 100 • 53 Bethel Road • Glen Mills, PA 19342
(610) 558-3332 • 1-800-505-6505

www.theclaytongroup.com



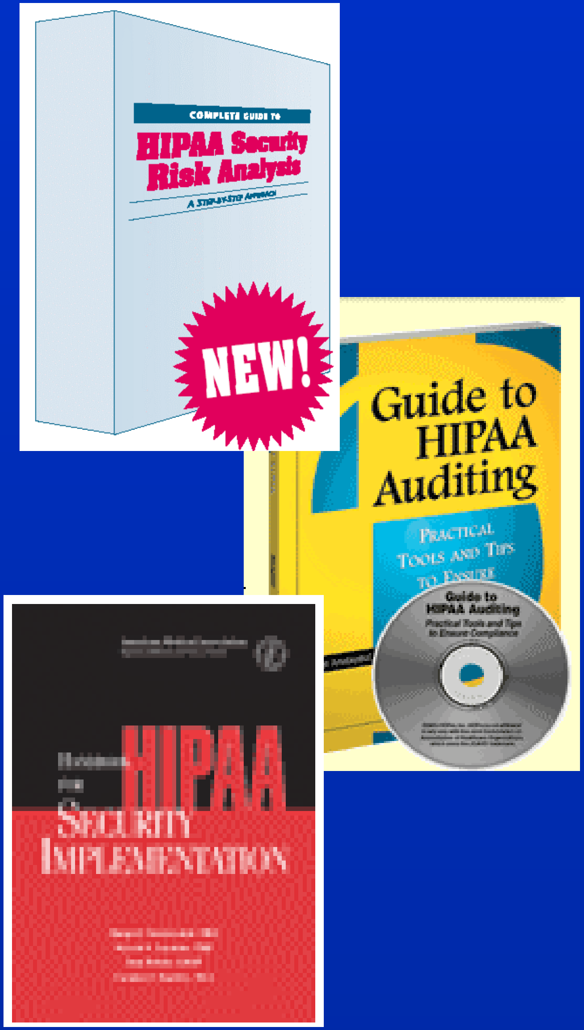
The Clayton Group HIPAA Security Template
Version 2.4

The Clayton Group

HIPAA Security P&P Checklist

	Administrative Safeguards	Have it already?	Customize Template	Refine with Team	Final Draft	Training Complete
1	General Guidelines to Safeguard Protected Health Information					
2	*Risk Analysis and Ongoing Risk Management*					
3	*Sanctions for Violating Privacy and Security Policies and Procedures*					
4	*Activity Review of Information System Security*					
5	*Assignment of Security Responsibility*					
6	Assignment and Management of Information Access Privileges					
7	Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems					
8	Training Program: Security Awareness and Training to Safeguard Electronic Protected Health Information					
9	*Security Incident Procedures: Response and Reporting*					

References & Resources


COMPLETE GUIDE TO
HIPAA Security Risk Analysis
A STEP-BY-STEP APPROACH
NEW!
Guide to HIPAA Auditing
Practical Tools and Tips to Ensure
Handbook for HIPAA Security Implementation

www.brownstone.com

- Amatayakul
- Lazarus

www.hcpro.com

- Amatayakul

https://catalog.ama-assn.org

- Amatayakul
- Lazarus
- Walsh
- Hartley

How good is your security ???

Why was I chosen ?

I was on vacation that day!

Thank you!

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

End of Session 2: Tuning up for HIPAA Compliance – Tips of the Trade

Session 3:

Establishing a Security Compliance Program

Angel Hoffman, RN, MSN

Director of Corporate Compliance, University of Pittsburgh Medical Center, Pittsburgh, PA