HIPAA Proposed Security Regulation Self-evaluation Tool

Holt Anderson, Executive Director
NC Healthcare Information & Communications Alliance, Inc.

www.nchica.org
**Introduction**

- **HIPAA EarlyView™** Version 1.0 is a self-administered tool that will assist an organization in assessing its readiness to comply with the proposed HIPAA Security Regulations.

- **HIPAA EarlyView™** can be used by:
  - Health plans
  - Healthcare providers
  - Clearinghouses
  - Public Agencies
  - Vendors
Development of *HIPAA EarlyView™*

- NCHICA is a 501(c)(3) nonprofit
- Members established HIPAA Implementation Planning Task Force in 1999
- Conceived by NCHICA HIPAA Data Security Work Group (providers, payer, state government, law firm, IT vendors, etc.)
- Developed over three months
- 521 questions track proposed Security Rule in sequence of implementation requirements / options
Organizations Included:

- Advisory Consulting Services
- Blue Cross & Blue Shield of North Carolina
- Cii Associates
- CertSite
- Data Dimensions, Inc.
- Duke University Health System
- Future HealthCare
- Interpath Communications
Organizations Included: (cont.)

- Keane
- NC DHHS - DIRM
- NC DHHS DMA (Medicaid)
- NC DHHS - DMH/DD/SAS
- Presideo
- UNC-Charlotte
- WakeMed
- Womble Carlyle Sandridge & Rice PLLC
Construction of Questions

- Teams assigned to develop questions according to 5 sections of proposed rule
- 10 readers commented on questions
- Work Group met to review comments and revise questions
- Team reached consensus on questions, their potential meaning and relevance to proposed implementation
Uses of **HIPAA EarlyView™**

- Staff education
- Gap analysis
  - Inadequate or missing policies
  - Previously unidentified vulnerabilities
- Due diligence documentation
- Budget planning
Critical Self-assessment

NOTE: Legal counsel should be consulted prior to deployment as data collected by HIPAA EarlyView™ may be subject to discovery proceedings or considered a public record.
NCHICA

HIPAA EarlyView

Version 1.0

HIPAA Security Proposed Regulation Self-Evaluation Tool

http://www.nchica.org
919-558-9258

Copyright 2000 NCHICA All Rights Reserved
License Agreement (per site)

License Agreement

HIPAA EarlyView™

COPYRIGHT / LICENSE / WARRANTY DISCLAIMER

NCHICA HIPAA EarlyView™ HIPAA Security Proposed Regulation Self-Evaluation Tool ["HIPAA EarlyView™" or the "Software"] Copyright © 2000 by the North Carolina Healthcare Information & Communications Alliance, Inc., Suite 200 Cape Fear Building, 3200 Chapel Hill/Nelson Blvd., PO Box 13048, Research Triangle Park, North Carolina 27709-3048 ["NCHICA"]. All rights reserved.

The Licensee should carefully read the following terms and conditions before using HIPAA EarlyView™. Your use of HIPAA EarlyView™ indicates your acceptance of this license agreement and warranty disclaimer ["Agreement"].

License

a) In consideration of a licensing fee as having been paid, NCHICA, Licensor, hereby grants a site-wide, nontransferable, nonexclusive, 99-year license, without right of sublicense (the "License") to use HIPAA EarlyView™ described in Exhibit A in accordance with this Agreement in object code only for Licensee’s own internal business purposes and for the

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved

Decline

Accept
Main Menu

HIPAA EarlyView™

- Start New Questionnaire
- Update Existing Questionnaire
- Run Reports
- About HIPAA EarlyView(TM)
- Exit

Copyright© 2000 NCHICA
All Rights Reserved
Start a New Questionnaire
Start a New Questionnaire

Enter New Questionnaire Name:

sample1

OK  Cancel
Enter Contact Data

**Contact Information Form**

**HIPAA Security Questionnaire Contact Data**

*Department Name: sample1*

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Division</td>
<td></td>
</tr>
<tr>
<td>Cost Center</td>
<td></td>
</tr>
<tr>
<td>Project Lead</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Address1</td>
<td></td>
</tr>
<tr>
<td>Address2</td>
<td></td>
</tr>
<tr>
<td>City</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
</tr>
<tr>
<td>Zip</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td></td>
</tr>
<tr>
<td>E-Mail</td>
<td></td>
</tr>
</tbody>
</table>

**Date Fields**

- **Start Date**: M/DD/YY
- **Due Date**: M/DD/YY
- **Facilitator**:            |
- **Title**:                  |
- **F. Phone**:               |
- **F. E-Mail**:              |
- **Serial #**:               |

*Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved*
Enter Contact Data

Contact Information Form

HIPAA Security Questionnaire Contact Data

Department Name: sample1

Organization: Org
Division: Div
Cost Center: CC
Project Lead: Proj Lead
Title: Title
Address1: Addr1
Address2: Addr2
City: City
State: ST
Phone: (999) 999-9999 Ext.
E-Mail: email@sample.com

Start Date: 1/1/00
Due Date: 12/31/00
Facilitator: Facilitator
Title: Title
F. Phone: (999) 999-9999 Ext.
F. E-Mail: facilitator@sampel.com
Serial #: 1234

Save and Close Form
HIPAA Questionnaire

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved
Update Questionnaire Menu

Update Existing HIPPA Questionnaire
for sample1

- Continue this Questionnaire
- Update Contact Information
- Return to Main Menu

Copyright © 2000 NCHICA All Rights Reserved
Security Questions

HIPAA Security Questionnaire

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

Question: 1
Questionnaire Name: sample1

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

Answer: Yes ☑ No ☐ N/A ☐ unanswered ☐
Due Diligence Demonstrated: ☐ Check if YES

Comments:
Refer To:
Document Name:
Doc Type:
Periodically Reviewed?:
Next Review Date (MM/DD/YYYY):
Point of Contact:
Contact Title:
Contact FAX:
Answer Date (M/D/Y):
Readiness Requirement:

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved
Security Questions

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

<table>
<thead>
<tr>
<th>Question</th>
<th>Questionnaire Name: sample1</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Answer</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Unanswered</th>
<th>Due Diligence Demonstrated:</th>
<th>Check if YES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments:</td>
<td>evaluation done by test org - June 1999</td>
<td>Refer To:</td>
<td></td>
<td></td>
<td>Document Name: tech eval</td>
<td></td>
</tr>
<tr>
<td>Document Name:</td>
<td>tech eval</td>
<td>Doc Type: Paper</td>
<td>Document Location:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodically Reviewed?:</td>
<td>No</td>
<td>Next Review Date (MM/DD/YYYY):</td>
<td></td>
<td></td>
<td>Contact Phone: (999) 999-9999 Ext. 1234</td>
<td></td>
</tr>
<tr>
<td>Point of Contact:</td>
<td>Mr. Contact</td>
<td>Contact E-Mail: <a href="mailto:boss@sample.com">boss@sample.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Title:</td>
<td>boss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact FAX:</td>
<td>(999) 999-9999</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Answer Date (M/D/Y):</td>
<td>6/9/00</td>
<td>Readdress Requirement:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Report Menu
Report Example

Answers by HIPAA Table

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>318</td>
<td>80</td>
<td>28</td>
<td>28</td>
<td>18</td>
</tr>
</tbody>
</table>

ANSWER KEY
1. Yes
2. No
3. N/A
4. Unanswered
# Questions answered with "NO"

<table>
<thead>
<tr>
<th>HIPAA Table</th>
<th>A</th>
</tr>
</thead>
</table>

**HIPAA Requirement**  
Certification

<table>
<thead>
<tr>
<th>HIPAA Implementation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Detailed Question</th>
<th>Refer To</th>
<th>Contact</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?</td>
<td>Susan Reference</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Report Example

## Question Listing by HIPAA Requirement and Implementation

<table>
<thead>
<tr>
<th>HIPAA Table</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Requirement</td>
<td>Certification</td>
</tr>
<tr>
<td>HIPAA Implementation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Detailed Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?</td>
</tr>
<tr>
<td>2</td>
<td>Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?</td>
</tr>
<tr>
<td>3</td>
<td>Does your organization maintain a technical evaluation history for BOTH information systems AND networks?</td>
</tr>
<tr>
<td>4</td>
<td>Does your organization require that BOTH information systems AND networks are reviewed after any additions or significant modifications to design?</td>
</tr>
<tr>
<td>5</td>
<td>Does your organization document all steps taken to ensure and maintain security compliance?</td>
</tr>
</tbody>
</table>

### HIPAA Requirement: Chain of Trust

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Detailed Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Does your organization require that a chain of trust partner agreement be signed with all third parties that process protected health information?</td>
</tr>
<tr>
<td>7</td>
<td>Does your organization explicitly state requirements for ensuring confidentiality and integrity of data in any chain of trust agreements?</td>
</tr>
<tr>
<td>8</td>
<td>Does your organization explicitly state requirements for availability of data in all chains of trust agreements?</td>
</tr>
<tr>
<td>9</td>
<td>Does your organization maintain the right to audit the security measures of third parties who process protected health information?</td>
</tr>
</tbody>
</table>
System Requirements

- Microsoft® Access® 97, Version 7 SR2
- Pentium® II with 32-64 megabytes RAM
- FreeZip or WinZip
- **Not supported** but FAQs on Web site
Associated Developments

- IBM Healthcare Group
- Raytheon
- Xcare and Boundary Information Group
- Others ???
IBM’s Enhancements

- Reduced and revised question set - 125
- Standardized terminology
- Emphasized regulatory consistency
- Recommended methodology that captures enterprise-wide variation
- Leveraged in IBM’s Fast Track HIPAA assessment
- Shared to support standard HIPAA tools
Raytheon Risk Management System

• Step 1: Survey Module
  – Incorporates HIPAA EarlyView™ dataset

• Step 2: Analysis Module
  – Reviews survey for risk
  – Graphically displays risk assessment results
  – Identifies and weights alternative courses of action
  – Manages implementation of selected actions
  – Permits “what if” analysis

• Step 3: Reports
  – Risk Assessment
  – Risk Management
  – Risk Relationship Cross-reference
  – Loss Expectancy
  – Compliance
Xcare
Boundary Information Group (BIG)

- Quick Start Assessment template that categorizes, prioritizes and maps to 80 compliance requirements
- ASP-based tool that has preloaded the Quick Start Assessment template and complete HIPAA EarlyView™ tool
  - manage risk exposure (assign resources and create mitigation strategies)
  - monitor compliance efforts (continuous reporting).
Available as Zipped file download on the NCHICA secure Web site

www.nchica.org
Thank you!

Questions ???