CCHIT is an independent, nonprofit organization with the mission of accelerating the adoption of robust, interoperable health IT by creating an efficient, credible certification process.
Four Goals of Certification

• Reduce the risks of investing in health IT
• Facilitate interoperability of EHRs and health information exchange networks
• Enhance availability of adoption incentives and regulatory relief
• Ensure that the privacy of personal health information is protected
CCHIT’s Role within the Broader Health IT Strategy

American Health Information Community and AHIC Workgroups

Office of the National Coordinator

Strategic Direction + Breakthrough Use Cases

CCHIT: Certifying Compliance of Health IT Products/Services

Harmonized Standards

Network Architecture

Privacy Policies

Certification of EHRs and Networks

Governance and Consensus Process Engaging Public and Private Sector Stakeholders

Accelerated adoption of robust, interoperable, privacy-enhancing health IT

Certification is a voluntary, market-based mechanism to accelerate the adoption of standards and interoperability
Development Process

**Step A: Environmental Scan**
- Use Cases and Standards
  - Element X
  - Priority as seen by stakeholders
  - Availability in the marketplace
  - Practicality of certification

**Step B: Develop Criteria**
- Criteria for 2008
  - Requirement X
- Roadmap for 2009, 2010 & beyond
  - 2009
  - 2010 & beyond
  - Future X
- Do not certify X

**Step C: Develop Test Scripts**
- Step-by-Step Test Scripts
  - Inspection Methods, Clinical Scenarios
  - Crosswalk

Public comment throughout the process.
Development Process

Step D: Pilot Test

- Call for Pilot Participation
- Selection of Participants
- Conduct Pilot Tests
- Refine Test Process and Scripts as Needed

Step E: Finalization

- Publish:
  - Proposed Final Criteria
  - Proposed Final Scripts
  - Pilot Results

- Make necessary refinements
- Publish:
  - Final Criteria
  - Final Test Scripts
  - Additional Guidance Materials

Launch Certification Program

Public comment

© 2008 | Slide 6 | 1/17/2008
Modular Certification Structure

Specialty Endorsement Criteria
- Cardiovascular Medicine: Additional Criteria and/or Specialized Case Scenario
- Future Specialty Additions

Population Care Criteria
- Child Health Criteria
- Ambulatory EHR Criteria
- Inpatient EHR Criteria
- ED EHR Criteria
- Future Population Additions, e.g. Behavioral Health
- Future EHR Domains e.g. Long Term Care

Domain Criteria

Foundation Criteria
- EHR Foundation Criteria (Interoperability, Security, Privacy, and Basic Supporting Functionality)
- Network Foundation Criteria (Interop, Security, Privacy, Basic Functionality)

Future Specialty Additions
Security Categories:

- Access Control
- Authentication
- Audit
- Technical Services
- Backup and Recovery
- Documentation
<table>
<thead>
<tr>
<th>Categories</th>
<th>Number of Criteria</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>S1 S2 S3 S4</td>
<td>4</td>
</tr>
<tr>
<td>Audit</td>
<td>S 5.2 S6 S7 S 8.1 S 8.2 S9 S 11</td>
<td>7</td>
</tr>
<tr>
<td>Authentication</td>
<td>S12 S13 S14 S15 S16.1 S16.2 S17 S18 S19 S20 S21 S22</td>
<td>12</td>
</tr>
<tr>
<td>Technical Services</td>
<td>S24 S25 S26 S27 S28 S29</td>
<td>6</td>
</tr>
<tr>
<td>Security Documentation</td>
<td>S23</td>
<td>1</td>
</tr>
<tr>
<td>Backup &amp; Recovery</td>
<td>R1 R2 R3</td>
<td>3</td>
</tr>
<tr>
<td>Reliability Documentation</td>
<td>R5 R6 R7 R9 R10 R11 R12 R13 14 R16 R17</td>
<td>11</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>44</td>
</tr>
</tbody>
</table>
## Criteria to Test Script Mapping

<table>
<thead>
<tr>
<th>Line #</th>
<th>Category and Description</th>
<th>Specific Criteria</th>
<th>Test Scripts Mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Security: Access Control</td>
<td>The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.</td>
<td>5.14, 5.15, 5.21, 5.24</td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td>The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.</td>
<td>5.19</td>
</tr>
</tbody>
</table>
Network Work Group

- 20 members
  - 9 HIEs
  - ONC
  - 3 Vendors
  - 7 Others
    - CDC, lab, state organizations, legal, industry experts
    - 6 at this meeting

- 25 Full Work Group Calls
  - 5 Subgroups for criteria development
  - 4 Subgroups for testing scenarios and methods

- Extensive coordination with Security, Privacy, and Interoperability Expert Panels
Status of Network Certification Development

- Environmental Scan
  - Published
  - Comments received

- 1st Draft of Criteria
  - Published
  - Comments received on December 22nd

- Test Scripts
  - Under development
  - Second phase will be formal scripts

- Alpha Test

- Pilot Test
Challenges of Network Certification

• Variability in HIEs
  – Services provided
  – Systems used

• State of the market
  – Early development
  – Financially constrained
  – In motion

• Requires testing of operational systems
  – Must accommodate different implementations
  – Must be practical within the HIE environment
Focus of 2008 Core Criteria

• Security
  – Transit
  – Non-repudiation
  – Audit logging
  – System authentication
  – Perimeter protection
  – Deactivation of users
  – Break the glass

• Total Criteria – 33

• Perimeter protection is not covered in other CCHIT security criteria
Focus of 2008 Modular Criteria

- Lab messaging as specified by HITSP
  - Must be capable of sending compliant messages
  - Not all messages must be compliant
  - 6 criteria
- CCD messaging
  - Must be capable of sending compliant messages
  - 1 criteria
- Query
  - Must be able to receive a query, retrieve data, and send response
  - 4 criteria
Network Certification
Overview of Changes

• Certification Structure
  – Core
  – 1 or more transaction
  – Query is an optional module

• Launch date for Network Certification
  – October 2008
Challenges of Testing

- Operational environment
- Trade offs of security approach
  - Documentation review
  - Physical testing
- Use of Laika tool for transaction testing
- Test script development is still underway
Upcoming Network Activities

• Market survey in January
• Participation in NHIN Collaborative Work Groups
• Development of testing methods, scenarios, and scripts