Privacy & Security Specialty Track Curriculum Competencies

Concepts to be interwoven throughout all levels of the curricula include:
- CRITICAL THINKING: For example the ability to work independently, use judgment skills effectively, be innovative by thinking outside of the box
- PERSONAL BRANDING: For example personal accountability, reliability, self-sufficiency

Specialty Track Student Learning Outcomes are derived from the CHPS credentialing exam content and are generally at a higher taxonomic level than similar learning outcomes from the associate level curriculum competencies as the intent of the specialty track is to build on the HIM academic foundation.

Completion of this specialty track does not alone enable a student to meet the CHPS exam eligibility criteria. However, the content when combined with work experience and other required education (where applicable), should assist in preparing students for the successful completion of the credentialing exam. See current CHPS eligibility requirements for additional information.

<table>
<thead>
<tr>
<th>Student Learning Outcomes</th>
<th>Bloom's Level</th>
<th>Curricular Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain I. Data Content, Structure and Standards (Information Governance)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Definition:</strong> Academic content related to diagnostic and procedural classification and terminologies; health record documentation requirements; characteristics of the healthcare system; data accuracy and integrity; data integration and interoperability; respond to customer data needs; data management policies and procedures; information standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subdomain I.C. Data Governance</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1. Facilitate development and verify maintenance of the inventory of software, hardware, and all information assets to protect information assets and to facilitate risk assessment. | 4 | • Data stewardship  
• Data and data sources for patient care  
• Management, billing reports, registries, and/or databases |
| 2. Create reasonable safeguards to reduce incidental disclosures. | 6 | • Data integrity concepts and standards |
| 3. Take part in the organizational risk assessment plan to identify threats and vulnerabilities. | 4 | • Data sharing  
• Data interchange standards (X2, HL-7)  
• Policy Application  
• Implement a systematic process to evaluate risk to and criticalities of information systems which contain PHI  
• |
| 4. Verify data backup plan. | 4 | • Data recovery plans  
• Data and computer security  
• Policies and Procedures  
• Disaster Preparedness Plan |
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 5. | Take part in development of guidelines, procedures and controls to ensure the integrity, availability and confidentiality of communication across networks (e.g. wireless, Internet, secure sockets, VPNs, and PKI). | 4 | • Bylaws  
• Provider contracts with facilities, medical staff by-laws, hospital by-laws  
• Enforce privacy and security policies, procedures, and guidelines to facilitate compliance with federal, state, and other regulatory or accrediting bodies |
| 6. | Recommend use of encryption of protected health information and other sensitive data based on risk assessment | 5 | • Data encryption standards; encryption software  
• Policies and procedures  
• Patient portal recommendations |

**Domain II. Information Protection: Access, Disclosure, Archival, Privacy and Security**

*Definition: Understand healthcare law (theory of all healthcare law to exclude application of law covered in Domain V); develop privacy, security, and confidentiality policies, procedures and infrastructure; educate staff on health information protection methods; risk assessment; access and disclosure management.*

**Subdomain II.A. Health Law**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | Evaluate and monitor facility security plan to safeguard unauthorized physical access to information and prevent theft or tampering. | 5 | • Healthcare legal terminology  
• Health information/record laws and regulations  
  - Consent for treatment, retention, privacy, patient rights, advocacy, health power of attorney, advance directives, DNR  
• Maintain a legally defensible health record  
• Subpoenas, depositions, court orders, warrants |

**Subdomain II.B. Data Privacy, Confidentiality and Security**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | Create a preventative program to detect, prevent and mitigate privacy/security breaches | 6 | • Internal and external standards, regulations and initiatives  
  - State and federal privacy and security laws  
• Patient verification  
  - Medical identity theft  
• Data security concepts  
• Security processes and monitoring  
• Security processes and policies  
• Data/information standards  
• Establish an incident/complaint investigation response, develop response plan, and identify team members to respond to a privacy or security incident  
• Develop policy and procedure for breach notification (federal)  
• Educate workforce on reporting requirements for breach |
| Subdomain II.C. Release of Information | 5 | notification (federal)  
- Perform risk assessment for breach notification (federal)  
- Manage contracts and business associate relationships and secure appropriate agreements related to privacy and security (e.g., BAA, SLA, etc.)  
-  
| Domain V: Compliance | 5 | Release patient specific data to authorized users  
- Create, document, and communicate information to include but not limited to minimum necessary protocols  
- Establish reasonable safeguards to reduce incidental disclosures and prevent privacy breaches  
- Access and disclosure policies and procedures  

**Definition:** COMPLIANCE activities and methods for all health information topics. For example, how to comply with HIPAA, Stark Laws, Fraud and Abuse, etc.; coding auditing; severity of illness; data analytics; fraud surveillance; clinical documentation improvement.

### Subdomain V.A. Regulatory

1. Manage the organization’s response to inquiries and investigations from external entities relating to privacy and security to provide response consistent with organizational policies and procedures.

| 5 | Internal and External standards regulations and initiatives  
- HIPAA, ARRA, The Joint Commission, Quality Integrity Organizations, CMS, meaningful use  
- Risk management and patient safety  
- Accreditation, licensure, certification  
- Legislative and regulatory processes  
  - Coding quality monitoring, compliance strategies, and reporting  

### Subdomain V.C. Fraud Surveillance

1. Develop performance measures and reports to monitor and improve organizational performance and report to appropriate organizational body.

| 6 | False Claims Act  
- Whistle blower, STARK, Anti Kickback, unbundling, upcoding  
- Role of OIG, RAC  
  - Fraud/Abuse  

2. Govern privacy and security policies, procedures, and guidelines to facilitate compliance with federal, state, and other regulatory or accrediting bodies.

| 6 | HIPAA  
- HITECH Act  
- Compliance systems  
- Bylaws  

---

1 This is the curriculum content floor, but not the ceiling.

Final Date: June 11, 2014
Rev. March 2, 2015
<table>
<thead>
<tr>
<th>Domain VI. Leadership</th>
<th>Supporting Body of Knowledge (Pre-requisite or Evidence of Knowledge)</th>
</tr>
</thead>
</table>
| **Definition:** Leadership models, theories, and skills; critical thinking; change management; workflow analysis, design, tools and techniques; human resource management; training and development theory and process; strategic planning; financial management; ethics and project management | **Pathophysiology and Pharmacology**  
**Anatomy and Physiology**  
**Medical Terminology**  
**Computer Concepts and Applications** |
| **Subdomain VI.H. Ethics** | **5**  
1. Recommend, review and approve protocols to verify, identify and access rights of recipients/users of health information.  
5. Professional and practice-related ethical issues  
   - AHIMA Code of Ethics  
   - Breach of healthcare ethics  
   - Cultural competence  
   - Healthcare professionals self-assessment of cultural diversity  
   - Self-awareness of own culture  
   - Assumptions, biases, stereotypes  
   - Diversity awareness training programs: age, race, sexual orientation, education, work experience, geographic location, disability  
   - Regulations such as ADA, ACLU |
|  |  
1. Security law requirements  
2. ARRA red flag rules  
3. Demonstrate privacy and security compliance with documentation, production and retention as required by State and Federal law as well as accrediting agencies  
4. Monitor compliance with the security policies and ensure compliance with technical, physical, and administrative safeguards  
5. Monitor and assess compliance with state and federal laws and regulations related to privacy and security to update organizational practices, policies, procedures and training of workforce  
6. Develop, deliver, evaluate and document training and awareness on information privacy and security to provide an informed workforce |
## Bloom's Taxonomy – Revised for AHIMA Curricula Mapping

<table>
<thead>
<tr>
<th>Taxonomy Level</th>
<th>Category</th>
<th>Definition</th>
<th>Verbs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remember</td>
<td>Recall facts, terms, basic concepts of previously learned material</td>
<td>Choose, Define, Find</td>
</tr>
<tr>
<td>2</td>
<td>Understand</td>
<td>Determine meaning and demonstrate clarity of facts and ideas</td>
<td>Collect, Depict, Describe, Explain, Illustrate, Recognize, Summarize</td>
</tr>
<tr>
<td>3</td>
<td>Apply</td>
<td>Use differing methods, techniques and information to acquire knowledge and/or solve problems</td>
<td>Adhere to, Apply, Demonstrate, Discover, Educate, Identify, Implement, Model, Organize, Plan, Promote, Protect, Report, Utilize, Validate</td>
</tr>
<tr>
<td>4</td>
<td>Analyze</td>
<td>Contribute to the examination of information in part or aggregate to identify motives and causes</td>
<td>Analyze, Benchmark, Collaborate, Examine, Facilitate, Format, Map, Perform, Take part in, Verify</td>
</tr>
<tr>
<td>5</td>
<td>Evaluate</td>
<td>Make judgments in support of established criteria and/or standards</td>
<td>Advocate, Appraise, Assess, Compare, Comply, Contrast, Determine, Differentiate, Engage, Ensure, Evaluate, Interpret, Leverage, Manage, Mitigate, Oversee, Recommend</td>
</tr>
<tr>
<td>6</td>
<td>Create</td>
<td>Generate new knowledge through innovation and assimilation of data and information</td>
<td>Build, Compile, Conduct, Construct, Create, Design, Develop, Forecast, Formulate, Govern, Integrate, Lead, Master, Propose</td>
</tr>
</tbody>
</table>

The layout for the levels and categories was adapted from Lorin W. Anderson and David R. Krathwohl’s *A Taxonomy For Learning, Teaching, and Assessing*, Abridged edition, Allyn and Bacon, Boston, MA 2001.
### CHPS Recommended Resources
**Source:** www.ahima.org

<table>
<thead>
<tr>
<th>Products</th>
<th>Content Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Program Management and Administration</td>
</tr>
<tr>
<td></td>
<td>Ethical, Legal, and Regulatory Issues, External Environment Assessment</td>
</tr>
<tr>
<td></td>
<td>Information Technology/Physical and Technical Safeguards</td>
</tr>
<tr>
<td></td>
<td>Customer/Client Patient Services</td>
</tr>
<tr>
<td></td>
<td>Investigation, Compliance, and Enforcement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Books</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nichols, C. Medical Identify Theft; Chicago: AHIMA press</td>
</tr>
<tr>
<td>Bowman, S. Health Information Management Compliance, Chicago AHIMA Press</td>
</tr>
<tr>
<td>E-Learning</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Privacy and Security Program</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Privacy and Security Institute (if applicable)</td>
</tr>
</tbody>
</table>

- All materials listed above will appear on the AHIMA store in the most recent newer version available.
Editorial Revisions made on 3.2.15
- Updated the title of the document.
- Added verbiage to top of the document: Completion of this specialty track does not alone enable a student to meet the CHPS exam eligibility criteria. However, the content when combined with work experience and other required education (where applicable), should assist in preparing students for the successful completion of the credentialing exam.