

Health Information Management CTAG and Alignment

This document contains information about three proposed Career-Technical Articulation Numbers (CTANs) for the proposed Health Information Management Services Career-Technical Assurance Guide (CTAG). The CTANs are:

1. Introduction to Health Information Management
2. Legal and Ethical Aspects of Health Information Management

CTAN #1: Introduction to Health Information Management:

CTAN alignment with the Tech Prep Health Information Management Services Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description: Students will be introduced to the fundamentals of health information management and health care data including legal health record components, policies and procedures associated with health record completeness and compliance, the health information management profession, patient and health care data and health information management’s role in survey readiness. Students will also discuss the various storage formats of health information including electronic health records.

Advising Notes: It is recommended that teachers of this course hold at least a bachelors degree (masters preferred) and minimum certification as a Registered Health Information Technician (RHIT). A career-technical student seeking credit under the terms of this CTAG must apply and be accepted to the college within three years of completing a career-technical education program/course or within the currency of the industry certificate or license.

Semester Credit Hours: 3 ALL LEARNING OUTCOMES ARE ESSENTIAL

Learning Outcomes The student will be able to:	Competencies in ODE’s Revised Career Field Technical Content Standards Dated October 2013.
1. Describe the health information management profession, the purpose and structure of the American Health Information Management Association and the certification process	1.1.2. Identify the scope of career opportunities and the requirements for education, training, certification, licensure, and experience. 1.1.4. Describe the role and function of professional

	<p>organizations, industry associations, and organized labor and use networking techniques to develop and maintain professional relationships.</p> <p>6.1.1 Define health information management (HIM) and differentiate among data, information and competency.</p>
<p>2. Identify the roles and responsibilities of health information professionals in the development of health record systems</p>	<p>6.1.1 Define health information management (HIM) and differentiate among data, information and competency</p> <p>6.1.2. Differentiate between primary and secondary health data sources and databases.</p> <p>6.1.3. Describe the architecture and data standards of health information systems.</p> <p>6.1.4. Describe the principles of structure, design, and use of health information (e.g. individual, comparative, reports, and trended data).</p> <p>6.1.5. Use health record data collection tools (e.g input screens, document templates).</p> <p>6.1.6. Recognize standard data definitions, vocabularies, terminologies, nomenclatures (e.g. SNOMED-CT), classifications (e.g. ICD9CM, ICD10, CPT), and/or relevant healthcare data sets (e.g. OASIS, HEDIS, UHDDS) as used in the organization's health information systems.</p> <p>6.1.7. Differentiate between the types and content of patient health records and the data collected (e.g. paper-based, electronic health records, and personal health records).</p> <p>6.1.8. Describe health record documentation requirements of external agencies and organizations (e.g. those specified by</p>

	<p>accrediting bodies, regulatory bodies, professional review organizations, licensure, reimbursement, discipline-specific “good practice”).</p> <p>6.1.9. Describe typical internal organizational health record documentation requirements, policies, and procedures.</p>
<p>3. Define the functions of the health record and its various components.</p>	<p>6.1.1 Define health information management (HIM) and differentiate among data, information and competency.</p> <p>6.1.2. Differentiate between primary and secondary health data sources and databases.</p> <p>6.1.3. Describe the architecture and data standards of health information systems.</p> <p>6.1.4. Describe the principles of structure, design, and use of health information (e.g. individual, comparative, reports, and trended data).</p> <p>6.1.5. Use health record data collection tools (e.g input screens, document templates).</p> <p>6.1.6. Recognize standard data definitions, vocabularies, terminologies, nomenclatures (e.g. SNOMED-CT), classifications (e.g. ICD9CM, ICD10, CPT), and/or relevant healthcare datasets (e.g. OASIS, HEDIS, UHDDS) as used in the organization’s health information systems.</p> <p>6.1.7. Differentiate between the types and content of patient health records and the data collected (e.g. paper-based, electronic health records, and personal health records).</p> <p>6.1.8. Describe health record documentation requirements of</p>

	<p>external agencies and organizations (e.g. those specified by accrediting bodies, regulatory bodies, professional review organizations, licensure, reimbursement, discipline-specific “good practice”).</p> <p>6.1.9. Describe typical internal organizational health record documentation requirements, policies, and procedures.</p>
4. Identify the various uses of the health records and its importance to each user	6.1.9 Describe typical internal organizational health record documentation requirements, policies and procedures.
5. Identify healthcare data, structure, content, and date sets commonly used in the healthcare field.	<p>6.1.1 Define health information management (HIM) and differentiate among data, information and competency</p> <p>6.1.2 Differentiate between primary and secondary health data sources and databases</p> <p>6.1.3 Describe the architecture and data standards of health information systems.</p> <p>6.1.4 Describe the principles of structure, design and use of health information (e.g. individual, comparative, reports, trended data)</p> <p>6.1.6. Recognize standard data definitions, vocabularies, terminologies, nomenclatures (e.g. SNOMED-CT), classifications (e.g. ICD9CM, ICD10, CPT), and/or relevant healthcare datasets (e.g. OASIS, HEDIS, UHDDS) as used in the organization’s health information systems.</p>
6. Apply organization-wide health record documentation guidelines	<p>6.1.5 Use health record data collection tools (e.g. input screens, document templates)</p> <p>6.1.9 Describe typical internal organization health record documentation requirements, policies and procedures.</p>
7. Apply policies and procedures to ensure organizational compliance with standards (accreditation, certification) and regulations	6.1.8 Describe health record documentation requirements of external agencies and organizations (e.g. those specified by accrediting bodies, regulatory bodies, professional review

<p>(legal, licensing).</p>	<p>organizations, licensure, reimbursement, discipline-specific good practice)</p> <p>6.1.10 Explain how to apply policies and procedures to ensure organizational compliance with regulations and standards including Medicare, Medicaid).</p>
<p>8. Maintain the accuracy and completeness of the patient record as defined by organizational policy and external regulations and standards.</p>	<p>6.1.9 Describe typical internal organizational health record documentation requirements, policies and procedures.</p> <p>6.3.4 Apply documentation management principals to ensure data quality, legal compliance, and integrity.</p> <p>6.3.5. Apply methods to ensure authenticity, timeliness, and completeness of health data entries in electronic information systems.</p> <p>6.3.6. Document profession-specific information in an EHR.</p> <p>6.3.7. Identify methods to correct errors entered in an EHR.</p>
<p>9. Describe the attributes and issues associated with electronic health records</p>	<p>6.3.1. Create and update documents within the EHR and PHR.</p> <p>6.3.2. Locate and retrieve information in the EHR and other electronic sources for a variety of purposes.</p> <p>6.3.3. Populate and use health data content.</p> <p>6.3.4. Apply documentation management principals to ensure data quality, legal compliance, and integrity.</p> <p>6.3.5. Apply methods to ensure authenticity, timeliness, and completeness of health data entries in electronic information systems.</p> <p>6.3.6. Document profession-specific information in an EHR.</p>

	<p>6.3.7. Identify methods to correct errors entered in an EHR.</p> <p>6.3.8. Access reference material available through an EHR.</p> <p>6.3.9. Identify the source of information entered in an EHR.</p> <p>6.3.10. Resolve minor technology problems associated with using and EHR.</p> <p>6.3.11. Follow access protocols for entry to an HER</p> <p>6.3.12. Manage documents within the EHR and PHR utilizing filing and patient identification methodologies.</p> <p>6.3.15 Describe the common insurance claim procedures and apply guidelines of documentation and processing to ensure federal, state and third-party insurance reimbursements are included and complete insurance claim forms.</p>
<p>10. Differentiate between the various formats to store and maintain health records and maintenance of these formats (paper, hybrid, electronic)</p>	<p>6.1.7. Differentiate between the types and content of patient health records and the data collected (e.g. paper-based, electronic health records, and personal health records.)</p>

1. CTAN #2 : Legal and Ethical Aspects of Health Information Management

CTAN alignment with the Tech Prep Health Information Management Services Pathway in the Career Field Technical Content Standards of the Ohio Department of Education. This CTAN contains all the learning outcomes of the OAN entitled “Legal Aspects” (OHL021) which is part of the Health Information Management TAG.

Course Description: Students will be introduced to the fundamentals of healthcare law including HIPAA Security and Privacy regulations. Students will discuss health information management ethics and health information management’s role in

maintaining the confidentiality and security of health information. Students will participate in release of information activities for confidential and non-confidential health information.

Semester Credit Hours: 2

Advising Notes: It is recommended that teachers of this course hold a master’s degree and certification of either Registered Health Information Technician (RHIT) or Registered Health Information Administrator (RHIA)

Alignment: All outcomes are essential

Learning Outcomes The student will be able to:	Competencies in ODE’s Revised Career Field Technical Content Standards, dated October 2013
<p>1. Differentiate between the types and sources of law, which constitute a basis for the use of health information in litigation.</p> <p>OHL021 LO #1</p>	<p>6.2.1. Identify components of the court systems and distinguish between public and private law, civil and criminal law and tort, contract actions, and the trial process.</p> <p>6.2.2. Differentiate between types of evidence used in healthcare litigation, process of discovery, and the permissible use of evidence in litigation, recognizing the elements of negligence and medical malpractice.</p>
<p>2. Apply regulatory policies and procedures as related to the HIPAA Security Regulations.</p> <p>OHL021 LO#10</p>	<p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p> <p>6.2.6 Use networks, including intranet, and internet, according to security and privacy policies and procedures.</p> <p>6.2.9 Implement administrative, physical and technical safeguards</p>
<p>3. Assess general legal principles governing access to confidential health information in a variety of circumstances.</p>	<p>6.2 Confidentiality, Privacy, and Security: Apply the fundamentals of confidentiality, privacy, and security to communicate health/medical information accurately and within legal/regulatory bounds across the organization and between organizations.</p> <p>6.2.4 Identify what constitutes the authorized access, release and</p>

<p>OHL021 LO#8</p>	<p>use of personal health data</p>
<p>4. Apply regulatory policies and procedures for access and disclosure of protected health information (PHI) as required by HIPAA privacy rules.</p> <p>OHL021 LO#11</p>	<p>6.2.4 Identify what constitutes the authorized access, release and use of personal health data</p> <p>6.2.5 Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT [HIPAA]).</p>
<p>5. Apply appropriate statutory requirements and/or applicable standards of practice to requests for access, use and disclosure of highly sensitive health information.</p> <p>OHL021 LO#12</p>	<p>6.2.4 Identify what constitutes the authorized access, release and use of personal health data</p> <p>6.2.5 Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT [HIPAA]).</p>
<p>6. Apply ethical standards and moral responsibility for protecting the privacy and confidentiality of health information.</p> <p>OHL021 LO#14</p>	<p>6.2.7 Maintain data integrity and validity within an information system</p> <p>6.2.8 Describe the possible consequences of inappropriate use of health data in terms of disciplinary action</p> <p>6.2.9 Implement administrative, physical and technical safeguards</p> <p>6.2.10 Describe elements that are included in the design of audit trails and data quality monitoring programs</p>
<p>7. Interpret legal issues related to obtaining consent for treatment by healthcare facilities and healthcare professionals.</p> <p>OHL021 LO#6</p>	<p>3.1.2 Maintain individuals' rights, respect individual's choices and obtain informed consent.</p> <p>6.2.4 Identify what constitutes the authorized access, release and use of personal health data</p>

<p>8. Distinguish between confidential and non-confidential information within a healthcare information system.</p> <p>OHL021 LO#7</p>	<p>6.2.4 Identify what constitutes the authorized access, release and use of personal health data</p> <p>6.2.5 Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT [HIPAA]).</p>
<p>9. Interpret laws, regulations, standards and ethics that govern and control the maintenance, disclosure and re-disclosure of confidential health information.</p> <p>OHL021 LO#9</p>	<p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p> <p>6.2.4 Identify what constitutes the authorized access, release and use of personal health data</p> <p>6.2.5. Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT [HIPAA]).</p>
<p>10. Distinguish between the components of the court system and trial process as related to the use of medical or health information in litigation.</p> <p>OHL021 LO#2</p>	<p>6.2.1. Identify components of the court systems and distinguish between public and private law, civil and criminal law and tort, contract actions, and the trial process.</p>
<p>11. Differentiate between types of evidence, process of e-discovery and the permissible use of evidence in litigation.</p> <p>OHL021 LO#3</p>	<p>6.2.2. Differentiate between types of evidence used in healthcare litigation, process of discovery, and the permissible use of evidence in litigation, recognizing the elements of negligence and medical malpractice.</p>

<p>12. Appraise elements of negligence as related to standards of practice for the healthcare facility and the healthcare professional.</p> <p>OHL021 LO#4</p>	<p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p>
<p>13. Report potential malpractice problems based upon the legal principles and standards of practice for healthcare professionals and/or facilities.</p> <p>OHL021 LO#5</p>	<p>6.2 Confidentiality, Privacy, and Security: Apply the fundamentals of confidentiality, privacy, and security to communicate health/medical information accurately and within legal/regulatory bounds across the organization and between organizations.</p> <p>6.2.1. Identify components of the court systems and distinguish between public and private law, civil and criminal law and tort, contract actions, and the trial process.</p> <p>6.2.2. Differentiate between types of evidence used in healthcare litigation, process of discovery, and the permissible use of evidence in litigation, recognizing the elements of negligence and medical malpractice.</p> <p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p> <p>6.2.4. Identify what constitutes the authorized access, release, and use of personal health data.</p> <p>6.2.5. Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT)</p>

	<p>[HIPAA]).</p> <p>6.2.6. Use networks, including intranet and internet, according to security and privacy policies and procedures.</p> <p>6.2.7. Maintain data integrity and validity within an information system.</p> <p>6.2.8. Describe the possible consequences of inappropriate use of health data in terms of disciplinary action.</p> <p>6.2.9. Implement administrative, physical, and technical safeguards.</p> <p>6.2.10. Describe elements that are included in the design of audit trails and data quality monitoring programs.</p>
<p>14. Interpret laws, regulations, and standards of practice as related to legal aspects of quality improvement, risk management and corporate compliance programs.</p> <p>OHL021 LO#13</p>	<p>6.2 Confidentiality, Privacy, and Security: Apply the fundamentals of confidentiality, privacy, and security to communicate health/medical information accurately and within legal/regulatory bounds across the organization and between organizations.</p> <p>6.2.1. Identify components of the court systems and distinguish between public and private law, civil and criminal law and tort, contract actions, and the trial process.</p> <p>6.2.2. Differentiate between types of evidence used in healthcare litigation, process of discovery, and the permissible use of evidence in litigation, recognizing the elements of negligence and medical malpractice.</p> <p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p>

	<p>6.2.6. Use networks, including intranet and internet, according to security and privacy policies and procedures.</p> <p>6.2.7. Maintain data integrity and validity within an information system.</p> <p>6.2.8. Describe the possible consequences of inappropriate use of health data in terms of disciplinary action.</p> <p>6.2.9. Implement administrative, physical, and technical safeguards.</p> <p>6.2.10. Describe elements that are included in the design of audit trails and data quality monitoring programs.</p>
<p>15. Assess the relevance of federal, state, and private sector initiatives related to the privacy, security and confidentiality of health information technology.</p> <p>OHL021 LO#15</p>	<p>6.2 Confidentiality, Privacy, and Security: Apply the fundamentals of confidentiality, privacy, and security to communicate health/medical information accurately and within legal/regulatory bounds across the organization and between organizations.</p> <p>6.2.1. Identify components of the court systems and distinguish between public and private law, civil and criminal law and tort, contract actions, and the trial process.</p> <p>6.2.2. Differentiate between types of evidence used in healthcare litigation, process of discovery, and the permissible use of evidence in litigation, recognizing the elements of negligence and medical malpractice.</p> <p>6.2.3. Explain and interpret regulatory requirements, standards of practice, legal responsibility, limitations, and implications of actions and describe the appropriate avenues for reporting incidences of malpractice or negligence.</p> <p>6.2.4. Identify what constitutes the authorized access, release, and</p>

	<p>use of personal health data.</p> <p>6.2.5. Distinguish between confidential and non-confidential information within the healthcare system and document, categorize, and prioritize requests for personal health information according to internal/external privacy and confidentiality guidelines (e.g., Health Insurance Portability and Accountability ACT [HIPAA]).</p> <p>6.2.6. Use networks, including intranet and internet, according to security and privacy policies and procedures.</p> <p>6.2.7. Maintain data integrity and validity within an information system.</p> <p>6.2.8. Describe the possible consequences of inappropriate use of health data in terms of disciplinary action.</p> <p>6.2.9. Implement administrative, physical, and technical safeguards.</p> <p>6.2.10. Describe elements that are included in the design of audit trails and data quality monitoring programs.</p>
--	---