Appendix A:
Reference Library

APPENDIX A: REFERENCE LIBRARY

PURPOSE: This reference library is intended to provide a focused subset of key papers, presentations, and other resources to aid readers in understanding the critical issues underlying the purpose of the Privacy and Security Solutions for Interoperable Health Information Exchange contract. This summary is not intended to be an exhaustive bibliography of all references related to privacy and security in electronic health information exchange.

Department of Health and Human Services (HHS) References

1. **Summary of Nationwide Health Information Network Request for Information Responses**, June 2005, HHS (www.hhs.gov/healthit/rfisummaryreport.pdf).

   Summary: A summary of the 512 responses to the Request for Information (RFI) received by the Office of the National Coordinator for Health Information Technology (ONC) in an effort to gain broad input regarding the best mechanisms to achieve nationwide interoperability to meet the goal of interconnecting clinicians so that they can exchange health information.

2. **Privacy and Security Solutions for Interoperable Health Information Exchange**, Request for Proposal No. AHRQ-05-0015, June 7, 2005, Agency for Healthcare Research and Quality (AHRQ)/ONC (http://www.ahrq.gov/fund/contarchive/rfp050015.htm).

   Summary: This is the Request for Proposal (RFP) underlying the HHS contract to assess and develop solutions to address the variation in organization-level business policies and state laws that affect privacy and security practices, including those related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification Provisions, which may pose challenges to interoperable health information exchange.

3. **The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care; Framework for Strategic Action**, July 21, 2004, Tommy Thompson, David Brailer, HHS (http://www.hhs.gov/healthit/frameworkchapters.html).

   Summary: This report, written by ONC to fulfill the requirements of Executive Order 13335, outlines a framework for development and implementation of a strategic plan to guide the nationwide implementation of health information technology in both the public and private sectors.

4. **HIPAA Administrative Simplification (Regulation Text)**, the complete privacy, security, and final enforcement regulation text (45 C.F.R. pts. 160, 162, and 164), unofficial version, as amended through February 16, 2006, HHS OCR (http://www.hhs.gov/ocr/AdminSimpRegText.pdf).

   Summary: This document brings together in one handy reference the HIPAA privacy and security regulations.

5. **Summary of the HIPAA Privacy Rule**, HHS Office for Civil Rights (OCR), May 2003 (http://www.hhs.gov/ocr/privacysummary.pdf).

   Summary: This is a summary, compiled by OCR, of key elements of the HIPAA Privacy Rule. It is not a complete or comprehensive guide to compliance, but it is often referred to as the best available and easiest to understand summary of the HIPAA Privacy Rule.

6. **Centers for Medicare & Medicaid Services (CMS) White Papers**, February 2006 (http://www.cms.hhs.gov/EducationMaterials/02_HIPAAMaterials.asp).

   Summary: The HIPAA Information Series for Providers, consisting of 10 papers, covers a number of important issues including covered entities, health plans, trading partners, and more.

Other Public and Private Organization References

1. **The Collaborative Response to the ONCHIT Request for Information**, from a collaboration of organizations including the American Health Information Management Association (AHIMA), the American National Standards Institute, the Center for Information Technology Leadership, Connecting for Health, eHealth Initiative, HL7, the Healthcare Information and Management Systems Society, and others, January 2005. (http://www.connectingforhealth.org/resources/collaborative_response/collaborative_response.pdf).

   Summary: On November 15, 2004, in an effort to gain broad input regarding the best mechanisms to achieve nationwide interoperability and exchange of electronic health information, ONC released an RFI. Thirteen major health and technology organizations developed this collaborative response endorsing a "Common Framework" to support health information exchange in the United States while protecting patient privacy.

2. **Ending the Document Game: Connecting and Transforming Your Healthcare Through Information Technology**, Commission on Systemic Interoperability, October 2005 (http://endingthedocumentgame.gov/).

   Summary: The Commission on Systemic Interoperability was authorized by the Medicare Modernization Act and established by the Secretary of Health and Human Services. Its members were appointed by the President and the Congress. The Commission was charged with developing a strategy to make health care information instantly accessible at all times, by consumers and their health care providers. This report documents the conclusions of the Commission.

3. **Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders**, July 2004, Markle Foundation, Robert Wood Johnson Foundation (http://www.connectingforhealth.org/resources/aech_exec_summary.pdf).

   Summary: A report that details specific actions the public and private sectors can take to accelerate the adoption of information technology in health care. The report contains recommendations in three categories: creating a technical framework for connectivity, developing incentives to promote improvements in health care quality, and engaging the American public by providing information to promote the benefits of electronic connectivity and to encourage patients and consumers to access their own health information.

4. **Regulatory and Policy Barriers to Effective Clinical Data Exchange: Lessons Learned from MedsInfo-ED**, Gottlieb et al., *Health Affairs*, September/October 2005 (http://content.healthaffairs.org/cgi/content/abstract/24/5/1197). [Note: Fee required for downloading.]

   Summary: MedsInfo-ED is a proof-of-concept clinical data exchange project that uses prescription claims data to deliver patient medication history to emergency department clinicians at the point of care. This patient safety initiative has uncovered numerous policy and regulatory barriers to successful clinical data exchange. The lessons learned and strategies to overcome the barriers are the focus of this paper.

5. **Emerging Trends and Issues in Health Information Exchange**, eHealth Initiative, 2005 (contact http://www.ehealthinitiative.org/ and request article).

   Summary: Selected findings from eHealth Initiative Foundation's Second Annual Survey of State, Regional, and Community-based Health Information Exchange Initiatives and Organizations.

6. **Health Information Technology Leadership Panel Final Report**, The Lewin Group, Inc., March 2005 (http://www.hhs.gov/healthit/HITFinalReport.pdf).

   Summary: In August 2004, The Lewin Group, a health care policy consulting firm, was retained by the National Coordinator for Health Information Technology (NCHIT) to convene the HIT Leadership Panel and report on its findings. The HIT Leadership Panel met in Washington, DC, on November 29, 2004. Panelists reviewed and commented on drafts of this report of their deliberations and approved the final report.

7. **An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule**, NIST Special Publication 800-66, National Institute of Standards and Technology, March 2005 (http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf).

   Summary: This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. It helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing and complying with the Security Rule. The publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule and does not supplement, replace, or supersede the HIPAA Security Rule itself.

8. **Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy**, Markle Foundation, Robert Wood Johnson Foundation, February 2005 (http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf).

   Summary: The linking of vital information as patients receive care from a fragmented health care system is a problem that has consistently plagued interoperability efforts in health care. The goal of the Linking Work Group was to address these issues, proposing practical strategies for improving health care through improved linking of information in a secure and efficient manner and in a way that allows health care professionals much improved access to needed information while respecting patients' privacy rights.

9. **National Consumer Health Privacy Survey 2005**, conducted for the California HealthCare Foundation by Forrester Research, Inc. (http://www.chcf.org/topics/view.cfm?itemID=115694).

   Summary: A groundbreaking study of Americans' attitudes and behaviors concerning health privacy, in order to investigate emerging consumer health privacy issues to inform and strengthen the national health information technology agenda.

Legal References

1. **Charting the Legal Environment of Health Information**, Rosenbaum et al., The George Washington University (GWU) School of Public Health and Health Services Department of Health Policy, May 2005 (http://www.rwjf.org/files/research/Legal%20Environment%20Long%20Version.pdf).

   Summary: This Policy Brief was part of a project supported by a grant from the Robert Wood Johnson Foundation that was designed to assess the legal environment for health information systems. The project also received support from AHRQ, which enabled the GWU team to convene periodic small meetings of legal and information experts in order to more closely examine the legal environment of the rapidly emerging electronic health information industry.

2. **Report of HIPAA Security Rule Work Group**, January 31, 2005, North Carolina Society of Healthcare Attorneys, Inc. (NCSHCA) (http://www.ncshca.org/securityrulereport013105.pdf).

   Summary: NCSHCA formed this work group to prepare a report to help lawyers in addressing how the HIPAA Security Rule affects law firms. This report provides a general overview of HIPAA requirements and how these requirements directly affect clients and indirectly affect law firms.

Websites and Portals

1. **Office of the National Coordinator for Health Information Technology (ONC)** (http://www.hhs.gov/healthit/) **and** (http://www.hhs.gov/healthinformationtechnology/).

   Summary: ONC provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety.

2. **American Health Information Community (AHIC)** (http://www.hhs.gov/healthit/ahic.html)

   Summary: A federally chartered commission to help advance efforts to reach President Bush's call for most Americans to have electronic health records by 2014. The AHIC provides input and recommendations to HHS on how to make health records digital and interoperable, and ensure that the privacy and security of those records are protected, in a smooth, market-led way.

3. **Agency for Healthcare Research and Quality (AHRQ)** (http://www.ahrq.gov/)

   Summary: AHRQ is the lead federal agency charged with improving the quality, safety, efficiency, and effectiveness of health care for all Americans. As one of 12

agencies within HHS, AHRQ supports health services research that will improve the quality of health care and promote evidence-based decision-making.

4. **AHRQ National Resource Center for Health Information Technology** (http://healthit.ahrq.gov/home/index.html).

   Summary: AHRQ created the AHRQ National Resource Center for Health Information Technology (the National Resource Center) to help the health care community make the leap into the Information Age. In addition to providing technical assistance, the National Resource Center shares new knowledge and findings that have the potential to transform everyday clinical practice.

5. **The eHealth Initiative** (http://www.ehealthinitiative.org/).

   Summary: The eHealth Initiative and the Foundation for eHealth Initiative are independent, nonprofit affiliated organizations whose missions are the same: to drive improvement in the quality, safety, and efficiency of health care through information and information technology.

6. **Connecting for Health** (http://www.connectingforhealth.org/index.html).

   Summary: Connecting for Health is a public-private collaboration under the direction of the Markle Foundation. It is designed to address the challenges of mobilizing health information to improve quality, conduct timely research, empower patients to become full participants in their care, and bolster the public health infrastructure.

7. **The University of Miami Ethics Programs: Privacy/Data Protection Project** (http://privacy.med.miami.edu/about_project.htm).

   Summary: The Privacy / Data Protection Project is a public education effort of the University of Miami Ethics Programs. The project's focus is on information protections in the health sector, particularly the HIPAA Privacy Rule and Security Rule. The site contains a set of free web-based HIPAA courses to meet the training requirements of these rules—linked to a glossary of more than 200 entries on privacy/security law and technology.

8. **Health Care Information and Management Systems Society (HIMSS) CPRI Toolkit: Managing Information Privacy & Security in Healthcare** (http://www.himss.org/asp/topics_cpriToolkit.asp?faid=78&tid=4).

   Summary: The CPRI Toolkit outlines general principles and provides best practices and examples of how health care providers should manage privacy and security. Sections of the CPRI Toolkit identify key activities to integrate into the process of managing information privacy and security.

9. **American Health Information Management Association (AHIMA), Health Information Exchange (HIE) Resource Tool Kit** (http://www.ahima.org/hie/index.asp).

   Summary: A web-based toolkit designed as a resource to assist individuals and organizations interested in participating in health information exchange initiatives.

10. **CMS HIPAA Resources** (http://www.cms.hhs.gov/HIPAAGenInfo/).

    Summary: Contains a comprehensive source of HIPAA-related resources including sections on guidance, health insurance reform, HIPAA Administrative Simplification, legislation, regulations and policies, and review boards.

11. **HHS OCR—HIPAA: Medical Privacy—National Standards to Protect the Privacy of Personal Health Information** (http://www.hhs.gov/ocr/hipaa/).

    Summary: Contains a comprehensive list of links to HIPAA-related privacy resources including sections on general background information, HIPAA regulations and standards, compliance and enforcement, educational materials, and a section specifically for consumers.

12. **National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)** (http://csrc.nist.gov/).

    Summary: CSRC's goal is to share information security tools and practices, provide one-stop shopping for information security standards and guidelines, and identify and link key security web resources to support the industry.

13. **International Organization of Standardization (ISO), Information Technology—Security Techniques—Code of Practice for Information Security Management**
    (http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=).

    Summary: ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in information security management. (Note: ISO/CD 27799, Health informatics—Security Management in Health Using ISO/IEC 17799, is currently under development.)

14. **American Health Lawyers Association** (http://www.healthlawyers.org/). [Note: Fee required for downloading.]

    Summary: The mission of the American Health Lawyers Association is to provide a forum for interaction and information exchange to enable its members to serve their clients more effectively; to produce the highest quality nonpartisan educational programs, products, and services concerning health law issues; and to serve as a public resource on selected health care legal issues.

15. **Davis Wright Tremaine, LLP** (http://www.dwt.com/practc/hit/bulletins/02-05_RHIOGovernance.htm).

    Summary: RHIO Governance Series: A Road Map for Establishing Your Health Information Organization. Until organizational, tax, and governance models for community or regional health information organizations (RHIOs) become standardized through practice or government dictate, founders of these organizations must determine the best form of entity, tax treatment, and governance structure for their fledgling organizations. While the form of the organization may vary, the process for establishing a RHIO is fairly straightforward and can be divided into the following 6 phases: (1) establishing the team, (2) data gathering and analysis, (3) formulating a

work plan, (4) strategic business planning, (5) model identification and analysis, and (6) addressing other legal issues.

16. **Electronic Privacy Information Center (EPIC)** (http://www.epic.org).

    Summary: EPIC is a public interest research center in Washington, DC. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

17. **Workgroup for Electronic Data Interchange (WEDI)** (www.wedi.org).

    Summary: WEDI's mission is to provide leadership and guidance to the health care industry on how to use and leverage the industry's collective knowledge, expertise, and information resources to improve the quality, affordability, and availability of health care. It is dedicated to improving health care through electronic commerce.