Appendix B:
Existing Guidance to Support
HIE Implementation Opportunities

APPENDIX B: EXISTING GUIDANCE TO SUPPORT HIE IMPLEMENTATION OPPORTUNITIES

There is an important opportunity for the states and territories to advance their own implementation strategies and simultaneously help ensure that they do not deviate too far from each other. While it is necessary and appropriate for each state or territory to implement the solutions suitable for its own circumstances, inconsistent solutions in key areas necessary for effective health information exchange (HIE) may raise new barriers to interstate activities and transactions. Reference to and use of nationally recognized guidance to support implementation should help minimize the risk of this kind of inconsistent development.

It has become clear through the Health Information Security and Privacy Collaboration (HISPC) reports that while the Health Insurance Portability and Accountability Act (HIPAA) may have brought some nationwide consistency to activities related to electronic health records (EHR) and health information exchange, it has also created some confusion. More significantly, the very flexibility which is necessary for HIPAA to apply to the full range of health care organizations within its scope, especially under the Security Rule, also limits its ability to serve as authoritative guidance in this area. HIPAA provides substantial value in EHR and HIE implementation by providing broad policy and procedural parameters and a nationally consistent compliance structure, but unavoidably leaves so much to the discretion of implementing organizations that it can only partially support implementation.

As the reports from states and territories participating in the HISPC project have made clear, current laws of almost all states do not supplement HIPAA substantially, if at all, in this area. While state law revisions to support EHRs and HIE feature in most solutions reports, it is generally impractical and perhaps counterproductive to embed specific business practices or technology requirements in legislation, and such an approach would increase the risk of interstate inconsistency. While the state law revisions proposed by many states may provide valuable supplemental guidance—especially if the various laws are consistent across the states, like HIPAA, these laws can only support implementation so far.

Additional guidance from other authoritative resources can also support implementation, however, and should be consulted by state implementation teams. There are a number of nationally authoritative resources available that may help with various aspects of implementation; if the same resources are consulted by different states facing the same issues, they are much more likely to implement consistent solutions.

We have identified the following nationally recognized, nonproprietary resources as potentially valuable for solutions implementation. This list is not intended to be exhaustive, but to identify existing guidance that may be valuable in supporting implementation. In

particular, the following sources provide valuable guidance that should be consulted in implementing EHR and HIE solutions:

- AHIMA, the American Health Information Management Association, the professional association for health information management professionals.
- CHC, the California HealthCare Foundation, a nonprofit foundation focused on improving the way health care is delivered and financed in California, by promoting innovations in care and broader access to information.
- CMS, the Centers for Medicare & Medicaid Services, a division of the US Department of Health and Human Services, which administers and supports the Medicare and Medicaid programs and is charged with enforcement of the HIPAA Security Rule.
- Connecting for Health, a program of the Markle Foundation intended to develop information technology for use in health and health care, while protecting patient privacy and the security of personal health information.
- eHealth Initiative, a national nonprofit organization intended to drive improvement in the quality, safety, and efficiency of health care through information and information technology.
- HealthKey, a collaboration of health care data sharing organizations, which developed a number of practices and principles for secure sharing of health information.
- HIMSS, the Healthcare Information and Management Systems Society, an international association focused on the use of health care information technology (IT) and management systems for the betterment of health care.
- NIST, the National Institute for Standards and Technology, a division of the US Department of Commerce, which develops and publishes information security guidance for federal agencies.

None of these resources provides complete support for implementation by any HISPC participant. They do, however, supplement HIPAA and other applicable laws and standards, and should help substantially advance implementation. Suggested guidance is identified by solution area, across the principal solution categories identified in the reports.

Governance

Most participants call for a permanent body to oversee and guide implementation of privacy and security solutions. The following resources may be helpful in implementing this kind of body.

- AHIMA, **Development of State Level Health Information Exchange Initiatives, Report and Work Book** (2006)
- AHIMA, **Surveying the RHIO Landscape: A Description of Current RHIO Models, with a Focus on Patient Identification** (2006)

- eHealth Initiative, **Connecting Communities Toolkit: Organization and Governance Module** (2006)
- Connecting for Health, **Financial, Legal and Organizational Approaches to Achieving Connectivity in Health Care** (2004)
- Ross, Tripathi, Anderson, McCutcheon and Stone, **NHII 2004—Governance Track Background Paper**

Legal and Regulatory Solutions

Most participants call for amending state law and introducing new legislation where required. The following resources may be helpful in developing such legislation.

- AHIMA, **Privacy and Security in Health Information Exchange** (2006)
- AHIMA, **Maintaining a Legally Sound Health Record—Paper and Electronic** (2006)
- AHIMA, **Homeland Security and HIM** (2005)
- AHIMA, **Laws and Regulations Governing the Disclosure of Health Information (Updated)** (2002)
- Center for Law & the Public's Health, **The Turning Point Model State Public Health Act State Legislative Table** (2004)
- Connecting for Health, **Common Framework P1: The Architecture for Privacy in a Networked Health Information Environment** (2006)
- National Committee on Vital and Health Statistics Letter to the Secretary of U.S. Department of Health and Human Services, **Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network** (June 22, 2006)
- Rosati and Lamar, **The Quest for Interoperable Electronic Health Records: A Guide to Legal Issues in Establishing Health Information Networks** (July 2005)
- Rosenbaum, Borzi, Repasch, Burke, and Benevelli, **Charting the Legal Environment of Health Information** (2005)

Business Practices and Policies Solutions

Most participants call for standardization of business practices and policies by adoption of model forms, policies, and processes, in areas including consent and authorization; application of federal law; exchange of sensitive information; and exchange of data related to Medicaid, public health, and law enforcement agencies. The following resources may be helpful in developing such materials.

- AHIMA, **Guidelines for Defining the Legal Health Record for Disclosure Purposes** (2005)

- AHIMA, **Identity Theft and Fraud—The Impact on HIM Operations** (2006)
- AHIMA, **Practice Brief: Understanding the Minimum Necessary Standard** (2003)
- AHIMA, **Practice Brief: Consent for Uses and Disclosures of Information** (2003)
- AHIMA, **Practice Brief: Required Content for Authorizations to Disclose** (2003)
- AHIMA, **Practice Brief: Regulations Governing Research** (2003)
- AHIMA, **Redisclosure of Patient Health Information** (2003)
- AHIMA, **Practice Brief: Defining the Designated Record Set** (2003)
- AHIMA, **Practice Brief: Implementing the Minimum Necessary Standard** (2002)
- Association of State and Territorial Health Officials, **Information Management for State Health Officials** (2004)
- Connecting for Health, **Common Framework P2: Model Privacy Policies and Procedures for Health Information Exchange** (2006)
- Connecting for Health, **Common Framework P3: Notification and Consent When Using a Record Locator Service** (2006)
- Connecting for Health, **Common Framework P6: Patients' Access to Their Own Information** (2006)
- Connecting for Health, **Common Framework P8: Breaches of Confidential Information** (2006)
- Connecting for Health, **Common Framework M1: Key Topics in a Model Contract for Health Information Exchange** (2006)
- Connecting for Health, **Common Framework M2: A Model Contract for Health Information Exchange** (2006)
- HealthKey Collaborative, **A Framework and Structured Process for Developing Responsible Privacy Practices** (2001)
- HealthKey Collaborative, **A Template for a Comprehensive Health Care Information Protection Agreement between Business Associates** (2001)
- Waller, **Ownership of Health Information in the Information Age** (1998)

Technological Solutions

Most participants call for standardized approaches to solutions for issues such as patient identification systems; information authorization, authentication, access, and audit;

segmenting data within electronic medical records; terminology standards; and transmission security standards. The following resources may be helpful in developing such solutions.

- AHIMA, **Data Standards, Data Quality, and Interoperability** (2007)
- AHIMA, **Using the SSN as a Patient Identifier** (2006)
- AHIMA, **Building an Enterprise Master Person Index** (2004)
- AHIMA, **Implementing Electronic Signatures** (2003)
- AHIMA, **Implementing Electronic Signatures, State Laws Appendix** (2004)
- AHIMA, **Facsimile Transmission of Health Information** (2006)
- AHIMA, **E-mail as a Provider-Patient Electronic Communication Medium and its Impact on the Electronic Health Record** (2004)
- AHIMA, **Provider-Patient E-mail Security** (2003)
- AHIMA, **A HIPAA Security Overview** (2004)
- AHIMA, **The 10 Security Domains** (2004)
- AHIMA, **Information Security-An Overview** (2003)
- AHIMA, **Security Risk Analysis and Management: An Overview** (2003)
- AHIMA, **Practice Brief: Security Audits** (2003)
- CMS, **Acceptable Risk Standards** (2004)
- CMS, **Information Systems Security Policy, Standards and Guidelines Handbook** (2004)
- CMS, **Information Security Levels** (2002)
- Connecting for Health, **Common Framework P4: Correctly Matching Patients with Their Records** (2006)
- Connecting for Health, **Common Framework T1: The Common Framework: Technical Issues and Requirements for Implementation** (2006)
- Connecting for Health, **Common Framework T2: Health Information Exchange: Architecture Implementation Guide** (2006)
- Connecting for Health, **Common Framework T3: Medication History Standards** (2006)
- Connecting for Health, **Common Framework T4: Laboratory Results Standards** (2006)

- Connecting for Health, **Common Framework T5: Background Issues on Data Quality** (2006)
- Connecting for Health, **Common Framework T6: Record Locator Service: Technical Background from the Massachusetts Prototype Community** (2006)
- HIMSS, **HIPAA Security Crosswalk** (2005)
- HIMSS, **Privacy and Security Toolkit: Managing Privacy and Security in Health Care** (2007)
- NIST SP 800-100, **Information Security Handbook: A Guide for Managers** (2006)
- NIST SP 800-94, **Guide to Intrusion Detection and Prevention Systems** (2007)
- NIST SP 800-92, **Guide to Computer Security Log Management** (2006)
- NIST SP 800-83, **Guide to Malware Incident Prevention and Handling** (2005)
- NIST SP 800-77, **Guide to IPsec VPNs** (2005)
- NIST SP 800-73, **Interfaces for Personal Identity Verification** (2006)
- NIST SP 800-66, **An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule** (2005)
- NIST SP 800-63, **Electronic Authentication Guideline** (2006)
- NIST SP 800-61, **Computer Security Incident Handling Guide** (2004)
- NIST SP 800-60, **Guide for Mapping Types of Information and Information Systems to Security Categories** (2004)
- NIST SP 800-47, **Security Guide for Interconnecting Information Technology Systems** (2002)
- NIST SP 800-45, **Guidelines on Electronic Mail Security** (2007)
- NIST SP 800-42, **Guideline on Network Security Testing** (2003)
- NIST SP 800-41, **Guidelines on Firewalls and Firewall Policy** (2002)
- NIST SP 800-40, **Creating a Patch and Vulnerability Management Program** (2005)
- NIST SP 800-36, **Guide to Selecting Information Technology Security Products** (2003)
- NIST SP 800-35, **Guide to Information Technology Security Services** (2003)

- NIST SP 800-34, **Contingency Planning Guide for Information Technology Systems** (2002)
- NIST SP 800-33, **Underlying Technical Models for Information Technology Security** (2001)
- NIST SP 800-30, **Risk Management Guide for Information Technology Systems** (2002)
- NIST SP 800-26, **Security Self-Assessment Guide for Information Technology Systems** (2001)
- NIST SP 800-14, **Generally Accepted Principles and Practices for Securing Information Technology Systems** (1996)
- NIST SP 800-12, **An Introduction to Computer Security: The NIST Handbook** (1995)
- NIST FIPS 200, **Minimum Security Requirements for Federal Information and Information Systems** (2006)
- NIST FIPS 199, **Standards for Security Categorization of Federal Information and Information Systems** (2004)
- U.S. Office of Management and Budget, **e-Authentication Guidelines for Federal Agencies** (2003)

Education and Outreach

All participants called for both consumer and provider education and outreach. Although limited resources are available for consumer education in particular, the following may be useful in addressing this solution.

- AHIMA, **HIPAA Privacy and Security Training** (2003)
- AHIMA, **Protecting Confidentiality in Health Care Education Programs** (2003)