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.

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)
- Center for Law & the Public’s Health, The Turning Point Model State Public Health Act State Legislative Table (2004)
- 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)
- 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)
Privacy and Security Solutions for Interoperable Health Information Exchange


**Technological Solutions**

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

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

- AHIMA, *Using the SSN as a Patient Identifier* (2006)
- Connecting for Health, Common Framework T5: Background Issues on Data Quality (2006)


- HIMSS, HIPAA Security Crosswalk (2005)


- NIST SP 800-77, Guide to IPsec VPNs (2005)

- NIST SP 800-73, Interfaces for Personal Identity Verification (2006)


- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy (2002)

- NIST SP 800-40, Creating a Patch and Vulnerability Management Program (2005)


**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.
