Recommendations

There is no single step that, if taken, would create a connected nationwide system of health information. This Commission has organized the steps needed to create such a system into three categories: adoption, interoperability, and connectivity. These categories were formed acknowledging the obvious overlap, but recognizing a need to structure recommendations to facilitate understanding.

Adoption focuses on the challenge of getting clinicians and consumers to use computer programs and information networks to maintain healthcare records, access relevant information about patient's background and illness, and offer support for safer, better decisions. Adoption includes the need to train doctors and other caregivers to ensure they are able to adopt these technologies effectively in their practices, provide technical support so clinicians do not need to become computer technicians, and make clinicians and consumers aware of the benefits and the privacy safeguards of these systems. The issues of adoption also require addressing the difficult economic and regulatory issues slowing investment and use of connected computer systems and the growing gaps between communities' access to these technologies.

Information is valuable when it is available as needed. **Interoperability** focuses on the need for healthcare information to be connected so information is accessible whenever and wherever it is needed and authorized. Interoperability issues often become exceedingly technical, focusing on the rules for how information is created, stored, and moved among computer systems.

Finally, there must be physical networks and operating rules for actually moving information around. **Connectivity** focuses on the networks providing the conduits for moving healthcare information seamlessly. A major obstacle to connectivity is creating a mechanism to connect an individual with his or her healthcare information. Connectivity also encompasses the major issue of consumer confidentiality—providing uniform privacy laws across the country and punishing those who seek to violate them.

In crafting these recommendations, the Commission focused on providing actionable advice. While the recommendations will possibly provoke debate in

some circles, the Commissioners, reflecting consensus and compromise, as well as a commitment toward action and the transformation of healthcare, present them with unanimous support.

To advance progress of the **adoption** of health information technology, the following actions should be taken:

1. **Adoption Incentives.** The Department of Health and Human Services (HHS) should implement, or seek authorization from Congress as necessary to implement, financial and other incentives for participation in a standards-based healthcare information network. These incentives should be directed toward individuals and organizations including healthcare providers, medical institutions, purchasers, and health plans. Incentives should include broad-based approaches such as pay-for-performance, as well as targeted approaches that include grants directed at small, safety net, and financially challenged providers. These incentives should begin to be implemented within two years. Employers and other private sector healthcare payers who will benefit from the adoption of interoperable healthcare information systems should be encouraged to provide similar incentives.

2. **Regulatory Reform.** The Secretary of HHS should act with urgency to revise or eliminate regulations that prevent healthcare entities, networks, hospitals, and clinicians from working together to create and adopt interoperable healthcare information systems, while promoting competition and maintaining reasonable protections against inurement and kickbacks. To ensure that healthcare providers can be confident in the legality of their actions, the Secretary should clearly state in the regulations those actions that are permissible and should direct the Centers for Medicare and Medicaid Services and the Office of the Inspector General to provide effective guidance to accelerate legally compliant activities that advance adoption of healthcare information technology. This effort should begin with 42 U.S.C. 1395nn, known as the Physician Self-Referral or Stark Law, and 42 U.S.C. 1320a-7b, known as the Federal Anti-Kickback Law, and regulations issued pursuant to those laws.

3. **Reporting on Adoption Gaps.** To ensure that the benefits of healthcare information technology are equally available to all the nation's citizens, HHS should monitor and annually issue a public report on gaps in the adoption

and effective implementation of interoperable healthcare information technology systems across all sectors of the nation's health system. The report should specifically identify types of gaps and should propose public and private sector policies to address and close those gaps.

4. **Workforce Needs and Impacts.** The Departments of Labor and Commerce, in concert with HHS, should identify and quantify deficiencies in healthcare workforce knowledge and skills that must be addressed in order to secure maximum benefit from healthcare information technology. The effects of healthcare information technology on the use of labor and the upward mobility of workers in the healthcare system should also be considered. Based on these findings, these Departments should create a plan to meet such workforce needs and better estimate the financial impact of workforce changes that occur as a result of effectively adopting healthcare information technology.

5. **Public Awareness.** HHS should develop and execute a public awareness campaign that helps educate consumers, providers, and other interested constituencies of the benefits of using interoperable health information technology and the steps they can take to realize those benefits. HHS should implement the campaign in conjunction with the Department of Commerce and other government and private-sector organizations.

The adoption of healthcare information technology has been hindered by the economics of healthcare. The Commission's recommendations seek to provide an incentive for adoption by rewarding the desired outcomes through pay-for-performance programs. In addition, direct financial and other support will be needed by small providers who get less direct benefit from use of the technology than larger providers and by safety net and other healthcare providers whose lack of financial resources have prevented their adoption of information technology.

Much of existing provider-based healthcare information technology is found inside hospitals. However, existing laws and regulations prevent hospitals from sharing those resources with other clinicians in the community. While these laws serve to protect competition among healthcare providers and to prohibit inappropriate payments to doctors, changes should be made to facilitate the sharing of information technology systems.

Information technology promises to help bring about an extraordinary transformation in healthcare. The Commission recognizes three foundational areas where these changes are not being adequately addressed. The use of information technology adds another dimension to the gaps in both healthcare's availability and quality. The first step in closing the gaps is to identify and quantify them. Using information technology effectively will require considerable changes in the way doctors, nurses, and other healthcare professionals practice medicine and approach their jobs. The Commission recommends a new focus on those changes, as well as on quantifying the benefits to healthcare workers from the implementation of information technology.

The second step is to deal directly with workforce issues. A shift to connected health information requires changes in practice by caregivers. It enables shifts in roles within the care team resulting in increased effectiveness and efficiency. It creates new roles for informatics experts and technical support personnel. The Commission recommends planning for these changes so that work force availability does not block adoption.

Finally, a critical dimension of this report is its focus on consumers. Consistent with the Commission charter, we recommend a concerted public education campaign to inform consumers and caregivers of the value and security of interoperable healthcare information systems.

To advance progress of the **interoperability** of health information technology, the following actions should be taken:

1. **Product Certification.** Purchasers of healthcare information technology products must have a reliable source of information about the interoperability, functionality, and security of these products; and vendors must be able to compete by differentiating their products beyond minimum standards. HHS should support a single, voluntary, private-public process to certify that products meet minimum standards. To ensure continual improvement in the products available to the healthcare community, the scope of certification activities should aggressively be expanded to include additional healthcare information technology products, and the minimum performance specifications should be augmented over time as technology and standards progress.

2. **Data Standards.** HHS, advised by the American Health Information Community (AHIC) and in consultation with the National Committee for Vital and Health Statistics (NCVHS), should ensure broad acceptance, effective implementation, and ongoing maintenance of a complete set of interoperable, non-overlapping data standards that function to assure data in one part of the health system is, when authorized, available and meaningful across the complete range of clinical, administrative, payment system, public health, and research settings. Additionally, AHIC should build upon the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to develop national standards for authentication, authorization, and security that will permit the necessary infrastructure for consumers' confident adoption of healthcare information technology.

3. **Standard Product Identifiers and Vocabulary.** Standardizing data at the point of its creation will greatly accelerate the creation of an interoperable healthcare information network. HHS should work with manufacturers of drugs, devices, and test kits to achieve standardized identifiers and vocabulary in labels and packaging, and in all data outputs of devices and test kits.

4. **Drug Records.** Interoperable healthcare information technology will ensure that all providers have access, when authorized, to their patients' medication records and will establish a robust capability for post-marketing surveillance of drugs. AHIC should, in its early activities, take a phased approach to developing a fully interoperable drug record for every American by 2010.

Interoperability of healthcare information can be achieved, but it will take more than good intentions or favorable marketing statements. Ensuring clinicians, hospitals, and other providers can purchase information technology systems enabling interoperability and appropriate functionality while protecting confidentiality requires an independent entity that can offer reliable product certifications. Certification depends upon the use of comprehensive, commonly accepted data, and technology standards—a critical infrastructure component not existing today but ready to be put into place rapidly through the work of AHIC. The Commission strongly endorses the creation of AHIC and the leadership demonstrated by HHS Secretary Mike Leavitt to chair and lead that entity.

Other industries have achieved interoperability by attaching computer readable information at the point of product manufacture. Manufacturers of retail products include a bar code with all the information needed to manage the product. Downstream participants in the supply chain use this information within their local systems. In healthcare, it is not yet practical to attach a physical tag to every drug or lab result with all the needed information. It is practical to identify the product with a standard identifier, to include that identifier in a national database, and to link it to all relevant information according to the appropriate terminology standard. The Commission recommends manufacturers of drugs, devices, and test instruments and kits identify the drug or result with standard identifiers and relay information in a standard vocabulary. The standardization of these items is the starting point to ensuring interoperability throughout the information supply chain.

Finally, we recommend, and in the body of the report provide the framework for an interoperable drug record for all Americans. This roadmap provides a management dashboard and coordinates choices, shows what needs to be done, and when each step needs to be completed to achieve this goal in a reasonable time. While this Commission could not, in 10 months, complete a roadmap for every dimension of healthcare information technology, the specific roadmap recommended for drug records can serve as a model for the development of other interoperable healthcare modules, such as a laboratory record, in the coming months.

To advance progress of the **connectivity** of health information technology, the following actions should be taken:

1. **Patient Authentication Standard.** Correctly aggregating and exchanging information about a specific person is essential and requires a uniform mechanism for authenticating the patient's identity. Congress should authorize HHS to develop a national standard for determining patient authentication and identity.

2. **Federal Privacy Standard.** Congress should authorize the Secretary of HHS to develop a uniform federal health information privacy standard for the nation, based on HIPAA and pre-empting state privacy laws, which anticipates and enables data interoperability across the nation.

3. **Nationwide Health Information Network.** A national healthcare information network is part of the critical infrastructure of national security. Therefore, HHS and its relevant agencies should coordinate and seek Congressional approval to coordinate, as necessary, with the Department of Homeland Security (DHS) and other cabinet Departments to ensure the nationwide health information network is created and receives funding commensurate with its contribution to the safety and security of the American public.

4. **Criminal Sanctions for Privacy Violations.** To augment the protections provided by HIPAA, Congress should authorize Federal criminal sanctions against individuals who intentionally access protected data without authorization.

5. **Consumer Protections.** Patients should be protected from the consequences of unauthorized access to or release of their healthcare information. Therefore HHS should study and recommend to Congress actions to prohibit discrimination based on data obtained in that way.

A uniform national approach to patient authentication was part of HIPAA. Creating a single, unique patient identifier would be the most direct way to establish patient authentication, and this approach is used throughout Europe. However, no approach to personal authentication in computer systems is free of financial costs, management issues, and privacy concerns. A direct approach would involve an administrative infrastructure that may be unacceptable to some at this time for a variety of reasons, including privacy concerns.

This approach could be modified to allow individuals to opt out of the uniform patient identifier. This compromise would let the nation provide a system benefiting individuals who recognize that their need for connected health information exceeds their privacy concerns while not penalizing those who find privacy more valuable. However, such a compromise would sharply reduce the administrative savings because the system would have to accommodate both sets of individuals. It would also present new liability challenges, specifically involving the potential liability of providers who lacked information in the treatment of a consumer whose information was not available.

An alternative to creating unique personal identification for everyone is to define a national standard set of authenticating information required to receive healthcare. This set of data could be captured when an individual first enters the healthcare system. Such information could include a set of data such as date of birth, school, employment, and insurance policy number.

Each of these approaches has strengths and weaknesses. The National Academies' Computer Science and Telecommunications Board's 2002 report, "IDs—Not That Easy," is a learned, post-9/11 look at the options from the perspective of national security. For purposes of healthcare and of national security, the time has come to select an alternative and eliminate the unacceptable cost of unconnected healthcare.

Much like the huge variety in patient authentication mechanisms, the variety and contradictions within the patchwork of state privacy laws also prevents the nation from connecting healthcare information. HIPAA set a minimum national privacy standard, but many states have augmented that standard. The resulting cacophony of state laws is fundamentally inconsistent: what is mandated in one state is prohibited in another. Congress must enact a uniform national privacy standard for the nation to realize the benefits of connected healthcare information.

The networks that will allow connected healthcare information are a critical national infrastructure, promoting the safe, efficient, and effective delivery of care; the protection of public health; the defense of the nation; and the promotion of rapid medical advancement. Without a connected health information network, the nation is slower in detecting epidemics of natural or man-made viruses and compromised in its ability to detect and recall defective drugs or medical devices. The healthcare field alone cannot carry the full burden of establishing the networks and infrastructure to connect healthcare information, and the Commission calls on DHS and other appropriate Federal agencies to assist in this essential task.

Finally, the Commission recognizes that no system of confidentiality and security protections will protect against all malicious attacks. To ensure the nation's reliance on the confidentiality of connected healthcare information, the Commission calls upon Congress to enact stiff criminal sanctions against individuals who purposefully access protected data without authorization. We also recommend providing clear and comprehensive safeguards against discrimination to protect anyone whose personal data were improperly released.