Report to the President

Revolutionizing Health Care Through Information Technology

President's Information Technology Advisory Committee

June 2004

Transmittal Letter

Members of the President's Information Technology Advisory Committee

Co-Chairs

Marc R. Benioff
Chairman and CEO
Salesforce.com, Inc.

Edward D. Lazowska, Ph.D.
Bill and Melinda Gates Chair
Department of Computer Science & Engineering
University of Washington

Members

Ruzena Bajcsy, Ph.D.
Director, Center for Information Technology Research in the Interest of Society (CITRIS) and Professor
University of California, Berkeley

Harold Mortazavian, Ph.D.
President and CEO
Advanced Scientific Research, Inc.

J. Carter Beese, Jr.
President
Riggs Capital Partners

Randall D. Mott
Senior Vice President and CIO
Dell Computer Corporation

Pedro Celis, Ph.D.
Software Architect
Microsoft Corporation

Peter M. Neupert
Chairman of the Board
Drugstore.com, Inc.

Patricia Thomas Evans
President and CEO
Global Systems Consulting Corporation

Eli M. Noam, Ph.D.
Professor and Director of the Columbia Institute for Tele-Information
Columbia University

Manuel A. Fernandez
Managing Director
SI Ventures/Gartner

David A. Patterson, Ph.D.
Professor and E.H. and M.E. Pardee Chair of Computer Science
University of California, Berkeley

Luis E. Fiallo
President
Fiallo and Associates, LLC

Alice G. Quintanilla
President and CEO
Information Assets Management, Inc.

Jose-Marie Griffiths, Ph.D.
Doreen E. Boyce Chair and Professor
School of Information Science
University of Pittsburgh

Daniel A. Reed, Ph.D.
Kenan Eminent Professor and Director,
Institute for Renaissance Computing
Department of Computer Science
University of North Carolina at Chapel Hill

William J. Hannigan
President
AT&T

Eugene H. Spafford, Ph.D.
Professor and Executive Director,
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University

Jonathan C. Javitt, M.D., M.P.H.
Senior Fellow
Potomac Institute for Policy Studies

David H. Staelin, Sc.D.
Professor of Electrical Engineering
Massachusetts Institute of Technology

Judith L. Klavans, Ph.D.
Director of Research
Center for the Advanced Study of Language and Research Professor
College of Library and Information Science
University of Maryland

Peter S. Tippett, M.D., Ph.D.
CTO and Vice-Chairman
TruSecure Corporation

F. Thomson Leighton, Ph.D.
Chief Scientist
Akamai Technologies

Geoffrey Yang
Managing Director
Redpoint Ventures

Health and Information Technology Subcommittee

Jonathan C. Javitt, M.D., M.P.H., Chair
Senior Fellow
Potomac Institute for Policy Studies

Peter M. Neupert, Co-Chair
Chairman of the Board
Drugstore.com, Inc.

David H. Staelin, Sc.D., Co-Chair
Professor of Electrical Engineering
Massachusetts Institute of Technology

Table of Contents

MEMBERS OF THE PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE III

HEALTH AND INFORMATION TECHNOLOGY SUBCOMMITTEE IV

TABLE OF CONTENTS V

OVERVIEW 2

FINDINGS AND RECOMMENDATIONS 10

PART I – PROMOTING THE ELECTRONIC HEALTH RECORD, CLINICAL DECISION SUPPORT, AND COMPUTERIZED PROVIDER ORDER ENTRY 10

1. *Economic Incentives for Investment in Health IT 10*
2. *Health Information Exchange 11*
3. *Facilitating the Sharing of EHR Technologies 12*
4. *Leveraging Federal Health IT Investments 13*
5. *Implementing a Standard Clinical Vocabulary 14*
6. *Standardized, Interoperable EHRs 17*
7. *The Human-Machine Interface and EHRs 18*
8. *Coordination of Federal NHII Development and Implementation 20*

PART II – PROMOTING SECURE, PRIVATE, INTEROPERABLE HEALTH INFORMATION EXCHANGE 21

9. *Unambiguous Patient Identification 21*
10. *Public Key Encrypted Internet Communications 22*
11. *Trust Hierarchy and Authentication 23*
12. *Tracing Access Requests 24*

APPENDIX I. PITAC HEALTH AND INFORMATION TECHNOLOGY SUBCOMMITTEE FACT-FINDING PROCESS 26

APPENDIX II: ACRONYMS 29

ACKNOWLEDGEMENTS 31

ABOUT THE PITAC AND THIS REPORT

The President's Information Technology Advisory Committee (PITAC) is appointed by the President to provide independent expert advice on maintaining America's preeminence in advanced information technology (IT). PITAC members are IT leaders in industry and academe with expertise relevant to critical elements of the national information infrastructure such as high-performance computing, large-scale networking, and high-assurance software and systems design. The Committee's studies help guide the Administration's efforts to accelerate the development and adoption of information technologies vital for American prosperity in the 21st century.

Chartered by Congress under the High-Performance Computing Act of 1991 (P. L. 102-194) and the Next Generation Internet Act of 1998 (P. L. 105-305), the PITAC is a Federal Advisory Committee. It is formally renewed through Presidential Executive Orders.

"Revolutionizing Health Care Through Information Technology," the current Committee's first report to the President and Congress, reflects the assessment of PITAC members that the overall quality and cost-effectiveness of U.S. health care delivery bear directly on the three top national priorities of national, homeland, and economic security established by the Administration. The PITAC concluded that although the potential of IT to improve the delivery of care while reducing costs is enormous, concerted national leadership is essential to achieving this objective. Numerous expert bodies have addressed the potential benefits to care providers and to individual Americans of applying IT to the complex, often life-critical – but increasingly antiquated, costly, and error-prone – paper-based realm of medical record-keeping. This report focuses on specific barriers to the nationwide implementation of health IT – barriers that can only be addressed by the Federal government.

Calling for Federal leadership to spur needed technological innovation, the PITAC report offers 12 specific recommendations for Federal research and actions to enable development of 21st century electronic medical records systems. At the core of such systems is the concept of a secure, patient-centered electronic health record (EHR) that: 1) safeguards personal privacy; 2) uses standardized medical terminology that can be correctly read by any care provider and incorporated into computerized tools to support medical decision making; 3) eliminates today's dangers of illegible handwriting and missing patient information; and 4) can be transferred as a patient's care requires over a secure communications infrastructure for electronic information exchange.

The report's findings and recommendations were developed by the Health and Information Technology Subcommittee of the PITAC during eight months of study. The subcommittee was briefed by both health care and IT experts in government and the private sector; reviewed the current literature; and gathered viewpoints at a town hall meeting of practitioners, researchers, and members of the public in conjunction with a major national meeting on health IT. The subcommittee's draft findings and recommendations were reviewed by the PITAC as a whole on April 13, 2004, and the final report was approved at its June 17, 2004, meeting.

OVERVIEW

…the most remarkable feature of this twenty-first century medicine is that we hold it together with nineteenth-century paperwork[1]

The U.S. health care system is acknowledged to be the world's most advanced scientifically and technologically. But amid multimillion-dollar diagnostic instruments, highly trained caregivers, and a vast facilities infrastructure, the most fundamental and pervasive basis on which Americans receive health care is the handwritten notation. Such notations not only form the record of a patient's interactions with a medical professional but also serve as the instructions for treatment, from prescriptions taken to a pharmacy to pre-operative and post-operative surgical procedures.

The paper-based techniques for record-keeping served caregivers and their patients well in earlier eras, when most people had a single physician over many years and much of their medical history resided in that physician's memory. In the modern era, however, the enormous complexity and sophistication of medical practice involving multiple care providers, the geographic mobility of citizens, and the critical requirement for adequate patient information in medical decision making have stressed the traditional modes to the breaking point. Indicators of distress in the health care delivery system have been visible for some time. Some examples:

- Medical errors, many of which can be prevented, are too common. In 2000, the Institute of Medicine estimated that 44,000 to 98,000 people die each year from medical errors in hospitals alone.[2] The magnitude and consequence of error in the outpatient setting is yet to be tallied.
- Medication errors have been found in one of every five doses given in typical hospitals and skilled nursing facilities, and 7 percent of those errors (more than 40 per day in a typical 300-patient facility)[3] were potentially life threatening.
- Health insurance costs have risen by over 10 percent in each of the past three years.[4]
- From 17 percent to 49 percent of diagnostic laboratory tests are performed needlessly because medical history and results of earlier tests are not available when new tests are ordered.[5,6]

---

[1] Secretary Tommy G. Thompson, remarks offered at the Health Information Technology Summit, Washington DC. May 6, 2004. http://www.hhs.gov/news/speech/2004/040506.html

[2] Institute of Medicine (IOM). *To Err Is Human: Building a Safer Health System*. The National Academies Press, 2000. http://www.nap.edu/openbook/0309068371/html/

[3] Barker K.N., Flynn E.A., Pepper G.A., et al. Medication errors observed in 36 healthcare facilities. *Archives of Internal Medicine.* 2002;162:1897-1903.

[4] The 2003 Kaiser Family Foundation and the Health Research and Educational Trust *Employer Health Benefits 2003 Annual Survey* found that increases in health insurance premiums were 10.9 percent, 12.9 percent, and 13.9 percent for 2001, 2002, and 2003 respectively. See http://www.kff.org/insurance/ehbs2003-1-set.cfm for details.

- There is no nationwide monitoring system to identify potential epidemics at an early stage, to identify patterns of adverse drug reactions, or to identify bioterrorist incidents in a timely manner.[7]

While these circumstances are well known, the root causes have not been clearly identified. In the Committee's view, the following factors head the list:

- The inherent limitation that individual caregivers cannot maintain every patient's full background information as well as current scientific and clinical best practice knowledge in their heads in order to make the best possible treatment decisions[8]
- The absence of necessary patient information and medical knowledge in the hands of decision makers at the point of clinical decision making
- An information recording system that relies heavily on human interpretation (e.g., handwriting, dosages)
- The rapid pace of medical advances, which overwhelms the ability of caregivers to keep up

The key to solving these problems is greater reliance on IT: to present the health care provider with appropriate patient information and medical knowledge at the point of clinical decision making; to record clinical concepts and events in standard, legible, and computable ways; and to check for potential errors in the decision-making process. Currently, most U.S. hospitals, outpatient settings, and other sites of care lack the kind of health IT infrastructure that would support these solutions.[9] Nationwide implementation of health information technology is the only demonstrated method of controlling costs in the long term without decreasing the quality of health care delivered.[10]

In his January 2004 State of the Union Address, President George W. Bush highlighted the importance of IT in health care when he stated, "By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care." The goal of this PITAC report is to help accelerate the adoption of IT in the health care sector by providing guidance to overcome

---

[5] Tierney W.M., McDonald C.J., Martin D.K., Hui S.L., and Rogers M.P. Computerized display of past test results: effect on outpatient testing. *Annals of Internal Mededicine*. 1987;107:569–74.

[6] Health Information Management Systems Society. "EHR and the Return on Investment." 2003. http://www.himss.org/content/files/EHR-ROI.pdf

[7] Regional projects are addressing these issues, but national monitoring is still in the future. See a recent example research project: Heffernan R., Mostashari F., Das D., Karpati A., Kulldorff M., Weiss D. Syndromic surveillance in public health practice, New York City. *Emerging Infectious Diseases*. May 2004. Available at: http://www.cdc.gov/ncidod/Eid/vol10no5/03-0646.htm

[8] G. A. Miller. The magic number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63:81-97, 1956.

[9] Recent surveys found that less than 14 percent of hospitals have CPOE systems and require physicians to use them and that approximately 16 percent of primary care physicians and 11 percent of specialists use an EHR in practice. See http://www.citl.org/research/ACPOE_Executive_Preview.pdf

[10] The Center for Information Technology Leadership (CITL) projects annual savings of approximately $44 billion with nationwide implementation of advanced ambulatory CPOE systems (which incorporate CDS). These savings are based on avoiding nearly 1.3 million outpatient visits and 190,000 hospital admissions, as well as more cost-effective medication, radiology, and lab ordering. See http://www.citl.org/research/ACPOE.htm

the principal technological barriers to moving in this revolutionizing direction. The Committee's general findings are that:

- Information technology can significantly reduce errors and costs[11],[12] while improving the quality of care received by patients in our health care system.
- Presidential leadership is essential to achieving the full potential of health information technology because multiple Federal departments and agencies must be coordinated in concert with the private sector, which delivers most of the care in our $1.6-trillion health care system.
- Advances in our communications and computational infrastructure are making wide adoption of health information technology feasible. Simultaneously, rising health care costs, an aging population, and increasing medical complexity make the adoption of health information technology vital and timely.

To address these findings, the PITAC proposes a framework (represented in Figure 1) for a 21st century health care information infrastructure and urges Federal leadership in making its development a key national objective. The four essential elements of this framework are:

- Electronic health records (EHRs) for all Americans that provide every patient and his or her caregivers all necessary information required for optimal care while reducing costs and administrative overhead
- Computer-assisted clinical decision support (CDS) to increase the ability of health care providers to take advantage of state-of-the-art medical knowledge as they make treatment decisions (called evidence-based medicine)
- Computerized practitioner order entry (CPOE) – such as for tests, medicine, and procedures – both for outpatient care and within the hospital environment
- Secure, private, interoperable, electronic health information exchange, including both highly specific standards for capturing new data and tools for capturing non-standards-compliant electronic information from legacy systems

---

[11] For a case study of implementation of electronic medical records and savings in an outpatient clinical setting, see Scott Barlow, Jeffrey Johnson, and Jamie Steck; "The Economic Effect of Implementing an EMR in an Outpatient Clinical Setting." *Journal of Healthcare Information Management*, Volume 18, No. 1, Winter 2004. http://www.allscripts.com/_resources/docs/wp/cur/JHIM_1_2004.pdf

[12] At one large academic hospital, the savings were estimated to be $5 million to $10 million annually on a $500 million budget. Another community hospital predicts even larger savings, with expected annual savings of $21 million to $26 million, representing about a tenth of its budget. In addition, in a randomized controlled trial, order entry was found to result in a 12.7 percent decrease in total charges and a 0.9 day decrease in length of stay. Even without full computerization of ordering, substantial savings can be realized. Data from LDS Hospital demonstrated that a program that assisted with antibiotic management resulted in a fivefold decrease in the frequency of excess drug dosages and a tenfold decrease in antibiotic-susceptibility mismatches, with substantially lower total costs and lengths of stay. See Bates D., Teich J., Lee J. et al. The impact of computerized physician order entry on medication error prevention. *Journal of the American Medical Informatics Association*. 1999; 6:313-21.

Figure 1. Framework for 21st Century Health Care Information Infrastructure

SURMOUNTING THE BARRIERS TO WIDESPREAD ADOPTION OF HEALTH INFORMATION TECHNOLOGY

Despite the availability and demonstrated results of IT solutions in health care,[13] widespread adoption of those solutions is hindered by a series of barriers: regulatory, technical (especially deployment), cultural, and financial (real or perceived). While this report addresses some of the most significant barriers for which Federal government action may be particularly appropriate, considerable research is needed into the nature of and solutions for others.

Medical Errors

Unlike most industries in which IT has improved efficiency, quality, and productivity, health care still operates using primarily paper-based records, phone calls, faxes, and mail. A patient's vital medical information is scattered across medical records kept in many different locations instead of being available at the time of care. Reports and x-rays are frequently misplaced, misfiled, or missing. Paper records are poorly suited for generating routine reminders to patients of needed immunizations or tests. Doctors must keep information about drugs, drug interactions, drugs covered by managed-care providers (formularies), clinical guidelines, and recent research in multiple computer systems, on paper, or in memory – a task that the exploding volume of relevant information makes nearly impossible. Handwritten medical orders and prescriptions are too often misunderstood. Errors have reached such levels that hospitals relying on paper charts and orders might legitimately notify their patients as follows:

> *Please be advised that this hospital uses manual, paper-based methods for tracking the process of your care and for implementing the orders of your physicians. Therefore, many orders that your doctors initiate will not be carried out as written. As a result, you may regrettably receive the wrong medicine, the wrong dose of the right medicine, the wrong route of administration, or possibly the correct medicine at the wrong time.*

Accelerating the adoption of information technology throughout the health care environment promises major benefits to consumers, caregivers, and those who pay for care. As President Bush has stated, health IT can save lives, reduce suffering, and make better use of resources.[14] A presentation to the PITAC given by Dr. Elias Zerhouni, Director of the National Institutes of Health, underscores the importance of a National Health Information Infrastructure (NHII) to the National Institutes of Health (NIH) Roadmap[15] goal of accelerating the pace at which new medical knowledge moves from the research laboratory to the patient's bedside.

---

[13] National Research Council, *Networking for Health: Prescriptions for the Internet.* Committee on Enhancing the Internet for Health Applications: Technical Requirements and Implementation Strategies, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Academies Press, Washington, D.C. 2000. http://books.nap.edu/catalog/9750.html

[14] U.S. President's Radio Address, January 24, 2004. http://www.whitehouse.gov/news/releases/2004/01/20040124.html

[15] NIH Roadmap at http://nihroadmap.nih.gov/index.asp

Unlike the nationalized health systems of many countries, however, the U.S. health care system is deliberately composed of private independent hospitals and physicians. While this arrangement has stimulated competition, maximized consumer choice, and provided ongoing incentives to excel and to innovate, the free market system does not inherently generate practical mechanisms for sharing information critical to patient care. There is no question that linking sites of care in a health information infrastructure can reduce duplicative services and unnecessary hospitalizations that occur because caregivers lack critical patient information located elsewhere. Unquestionably, electronic health records and computerized order entry tools markedly reduce medical errors and adverse drug events. However, that linkage must span the diverse information systems of multiple unrelated caregivers and institutions that are inherently in competition with one another.

Advances in health information technologies have already proven themselves in the care of America's veterans and military personnel. For example, Veterans Administration hospitals have reduced the rate of incorrectly administered medications from 1 in 20 ambulatory care prescriptions to less than 1 in 100,000. Simultaneously, the annual cost of care per eligible veteran has decreased by nearly half. The military has pioneered the use of electronic health records and physician decision-support systems, combined with electronic tools, to involve the patient in the care-giving process. These initiatives have reduced hospitalizations and markedly improved all critical benchmarks in patients suffering from respiratory disease, congestive heart failure, diabetes, and other chronic conditions.[16]

Reducing Costs

Inherent in the deployment of technology is the challenge of paying for it and creating incentives for using it efficiently. Many hospitals and physicians may have the capital to invest in and implement IT systems, provided that they are confident the systems and standards are sufficiently mature not to render their investments soon obsolete. However, the current payment system does not provide incentives to make the investment, since many benefits of an effective health information system go primarily to patients and to those who pay for their care, rather than to the hospitals and doctors who invest in the hardware, software, and training. The most critical part of a national infrastructure – the facility for exchange of health information among hospitals, physicians, and other providers – offers some benefit to individual caregivers, but this infrastructure primarily benefits patients, payers, and society.

Many private and governmental groups are participating in the development of our NHII, but the pace of progress could be significantly accelerated by the Federal actions advocated in this report. The long-term vision for the NHII, expressed by the Department of Health and Human Services (HHS) and others, is of a totally interconnected electronic information infrastructure supporting health care: all information about a patient from any source could be securely available to any health care provider when needed, while assuring patient control over privacy.

[16] Presentation to the PITAC by Anthony Principi, Secretary, and Jonathan Perlin, Deputy Undersecretary for Health, Department of Veterans Affairs (VA), November 2003.

Applying Lessons Learned From Advances in Other Fields

Many health information technology challenges echo IT issues in other fields. Wherever possible, the research and development (R&D) effort should be shared. In the PITAC's view, it is critical that the Federal departments and agencies focused on health care take maximum advantage of solutions that have already been developed. Possible models, in particular regarding computer infrastructure, privacy, and security, may be found where there is a long history of research, such as at the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Defense Advanced Research Projects Agency (DARPA), the Department of Energy (DOE), and other agencies in the multiagency Networking and Information Technology Research and Development (NITRD) Program. Existing information sources that should also be taken into account when considering solutions are a National Research Council report on security and privacy[17] and the report of the Computing Research Association (CRA) Grand Challenges Conference on Trustworthy Systems.[18] Two of the four challenges identified by the CRA report apply directly to health IT: building large-scale, distributed, reliable computing systems and providing user control over security and trust.

Education and Training of Health Care Professionals

While many of the recommendations in this report are technical in nature, the PITAC understands that technology cannot be adopted successfully without extensive education and training. The 2001 PITAC report to the President on health IT called for incentives to develop a cadre of medical professionals with sufficient expertise to develop these training programs. [19] The PITAC recognizes the importance of that recommendation. Moreover, as the community demonstration projects the PITAC proposes grow and thrive, the learning and successful methods must be shared with other communities and the general public.

Privacy and Security of Electronic Health Records

The PITAC recommendations in this report are fully cognizant of and compatible with the provisions of the Health Insurance Portability and Accountability Act (HIPAA). A robust NHII will require a firm foundation of trust. Americans must be assured that their confidential health information will not be misused and that there are adequate legal remedies in the event of inappropriate behavior on the part of either authorized or unauthorized parties. The HIPAA and its subsequent rule making have provided that framework - a framework that will continue to evolve as the challenges of implementing the NHII are addressed.

NITRD R&D

The 11-agency NITRD Program is the Federal government's principal locus of fundamental research and development in advanced information technologies, including high-

---

[17] National Research Council, *For the Record: Protecting Electronic Health Information. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure*, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Academies Press, Washington, D.C. 1997. http://www.nap.edu/readingroom/books/ftr/

[18] CRA Conference on "Grand Research Challenges in Information Security & Assurance." Airlie House, Warrenton, VA. November 16-19, 2003. http://www.cra.org/Activities/grand.challenges/security/home.html

[19] *Transforming Health Care Through Information Technology*, President's Information Technology Advisory Committee, February 9, 2001. http://www.nitrd.gov/pubs/pitac/pitac-hc-9feb01.pdf

end computing components and software; wired, wireless, and hybrid high-speed networking; development of software and software-intensive systems; human-computer interaction and information management technologies; and social and economic implications of information technology. Most recommendations made in this report are targeted for health information technology research and development that is part of the NITRD Program, particularly R&D administered through the Agency for Health Care Research and Quality (AHRQ) and the National Institutes of Health (NIH), both part of HHS.

More broadly, however, the coordinated IT research portfolio of the NITRD agencies provides a rich and diverse assortment of R&D activities and new technologies across the spectrum of information technologies that could be extremely helpful in developing the health care capabilities discussed in this report. Many of the technical barriers described represent pervasive IT issues, particularly those inhibiting the deployment of secure, interoperable information exchange. The PITAC urges the Federal health care agencies to join in the interagency efforts to respond to these overarching IT issues.

For example, a recent report of the NSF Blue Ribbon Advisory Panel on Cyberinfrastructure recommended that NSF establish and lead a large-scale, interagency, and internationally coordinated Advanced Cyberinfrastructure Program (ACP) to create, deploy, and apply cyberinfrastructure in ways that radically empower all scientific and engineering research and allied education.[20] The same issues need to be addressed in promoting the deployment of a secure, private, interoperable health information exchange infrastructure. Efforts to resolve the issues in doing so need to be coordinated across all Federal agencies. This report emphasizes areas where, in the PITAC's view, the NITRD Program has opportunities to accelerate development and deployment of private and secure electronic health records and related health information technology across the United States.

[20] The full report of the Advisory Panel is available at http://www.cise.nsf.gov/sci/reports/toc.cfm

FINDINGS AND RECOMMENDATIONS

The PITAC's findings and recommendations are grouped into two parts. Part I focuses on EHRs, computer-assisted clinical decision support, and computerized order entry. Part II focuses on secure, private, interoperable electronic health information exchange. There is a great deal of overlap in these recommendations, indicating the degree to which core elements are inherently interrelated.

Part I – Promoting the Electronic Health Record, Clinical Decision Support, and Computerized Provider Order Entry

1. Economic Incentives for Investment in Health IT

Finding:

Investment in health IT by physicians, hospitals, and other caregivers is inhibited because much of the benefit is perceived to flow to external parties, primarily payers. There are no reliable studies that document the returns on such investments to providers, payers, patients, and society. The incentive to invest in systems that exchange health data among potentially competing caregivers is even less well documented and there may be perverse economic incentives that inhibit such investment, despite clear evidence of improved safety and reduced duplication of services. In addition, potential government investment is hampered by lack of sufficient economic information to document and score resulting savings to the Federal budget.

Recommendation:

Increase Federal support for demonstration-based studies that quantitatively measure all major costs and benefits of public and private NHII and EHR investments and practices. Where benefits are not directly returned to those who must invest in IT solutions, Federal means should be sought for redressing the imbalance. One approach that should be studied is that of adopting reimbursement incentive structures that reward the use – rather than merely the installation – of EHR systems, health information exchange, electronic order entry, and computerized decision support under Medicare and other Federal health care programs. Approaches should also be identified to encourage private payers to provide similar incentives and to measure the impact of those incentives.

Discussion:

Financially stressed caregiver organizations, and even those not so financially stressed, often hesitate to invest in IT solutions because of a broad perception within these organizations that they receive little financial benefit from the improved quality and safety associated with health IT under current public and private reimbursement policies. Although there are clear potential benefits associated with reducing the burden of managing paper records, reducing medication errors to shorten hospital stays, and similar outcomes of computerization, there are no compelling economic studies – controlled or otherwise – to guide the community. The resulting uncertainty and lack of evidence concerning return on investment (ROI) has slowed IT investment decisions in the private sector. Conversely, in Federally funded hospitals – most

notably the Veterans Health Administration, where payer and caregiver are combined – universal adoption of health IT systems began more than a decade ago.

The effectiveness of investment in IT solutions would be enhanced by the availability of better information on the costs and benefits of alternative architectures and system choices. Competitive, peer-reviewed development and demonstration efforts that document the benefits of health IT investment to patients, providers, payers, and society are critical to moving forward. This may be achieved by an expansion of programs already conducted by units within HHS – AHRQ and the Office of the Assistant Secretary for Planning and Evaluation (ASPE). However, input into the design of such research should be sought from the Council of Economic Advisers (CEA), the Office of Management and Budget (OMB), the Congressional Budget Office (CBO), and the General Accounting Office (GAO) so the findings will maximally inform public policy. The findings will support appropriate scoring of the resulting budgetary savings under the rules currently in place at OMB and CBO.

2. Health Information Exchange

Finding:

Although local EHR systems are beginning to proliferate, the exchange of data among these systems is essential when significant numbers of patients receive care from several unrelated caregivers. While fully standardized, interoperable EHR systems remain a long-term goal, the need for health information exchange among caregivers must be addressed now. Diverse, inclusive, regional or statewide demonstrations of health information exchange involving multiple private (or Federal) caregivers are essential steps to national deployment and would address immediate, serious needs.

Aside from EHR systems, patient information that is essential to proper care is already contained in numerous existing hospital administrative systems and pharmacy, laboratory, and diagnostic facility systems. Pilot demonstrations have proven the feasibility of providing local caregivers with immediately viewable, non-standardized data (data reported in a form that cannot be compared and analyzed computationally) in rapid, cost-effective deployments. As underlying information systems become increasingly standards-based in the future, the exchanged data will become increasingly interoperable and valuable. Further research and development are needed to resolve many technical and procedural issues and broader, statewide and regional demonstrations are needed to resolve scalability and acceptability issues.

Recommendation:

Increase Federal support for community and regional demonstrations of health information exchange that can draw upon and provide remote viewing of existing data sources, many of which do not conform to highly specific data standards. R&D is needed to devise standard ways to present information that help clinicians integrate disparate data from multiple sources. The Federal government should coordinate these activities across the relevant agencies including HHS (including the Food and Drug Administration [FDA]), Department of Defense (DoD), NIST, and NSF.

Discussion:

Although many stand-alone EHR systems exist, they provide only limited value unless they can share data across sites of care because many patients appear at multiple sites without records

in hand. Federated models for access to viewable EHR data preserve caregiver control of patient information while achieving most of the data-interchange benefits of large centralized databases.

There has long been a constituency advocating completely standardized data as a prerequisite to successful information exchange. An example is the move to standardize the names of all laboratory tests, so that values obtained from multiple laboratories on a given patient can be displayed graphically. In contrast, when laboratory tests are denoted by different names, or their values are stored in different numerical formats, computer systems are less able to aggregate data. However, caregivers assert that, since they are trained to understand the differences in nomenclature, immediate access – even to non-standardized data – offers them most of the benefit of completely standardized data. This is the motivation for much of the health care provider participation in the effort to set a Continuity of Care Record (CCR)[21] standard under ASTM International.[22] This goal can be achieved through an expansion of funding for existing programs conducted by AHRQ and the ASPE Office of National Health Information Infrastructure. The Federal government should also coordinate these activities across other relevant agencies, including HHS and FDA, DoD, NIST, and NSF.

3. Facilitating the Sharing of EHR Technologies

Finding

In many communities, hospitals and other facilities that are beginning to deploy EHR systems are constrained from sharing those systems with referring physicians and other community entities by current interpretations of anti-fraud and anti-kickback laws. Not only are many of the most constraining interpretations generated outside of the legislative process, much of the constraint stems from interpretations drawn at the local level by compliance officers seeking to protect their institutions from possible violations. In the drafting of those laws, there was clearly no legislative intent to hamper the sharing of health information with its clear benefit to patients.

Recommendation

Promptly convene a Federal rapid-response task force under the direction of the new National Health Information Technology Coordinator to identify actual and perceived legal impediments to sharing of EHR systems by physicians, hospitals, laboratories, and pharmacies. That task force should include medical, legal, and economic expertise and representation from the Office of the Inspector General (OIG)/HHS, the Office of the General Counsel (OGC)/HHS, the Department of Justice (DOJ), and the General Accounting Office (GAO). The task force should produce clear guidance that is widely accepted by all branches of Government and private

---

[21] A brief paper describing the CCR is available at Web site of the ASTM (originally known as the American Society for Testing and Materials) Committee E31 on Healthcare Informatics: http://www.astm.org/COMMIT/COMMITTEE/E31.htm ASTM E31 has about 270 members and develops standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of information used within health care and health care decision making, including patient-specific information and knowledge.

[22] ASTM International is one of the largest voluntary standards development organizations in the world (more than 30,000 technical expert members who represent producers, users, consumers, government, and academia from more than 100 countries).

agencies and that maximally benefits the populace by facilitating the deployment of health IT solutions.

Discussion

Both the executive and legislative branches of the Federal government clearly desire to accelerate the deployment of health IT in order to reduce medical errors, save lives, improve the quality of care, and maximize the efficiency of health care. The unintended consequences of laws designed for other purposes (anti-fraud, anti-kickback) can be examined only from a multidisciplinary perspective. The scientific approach ordinarily is not applied to the manner in which legislation is implemented in the rule making process and in which that rule making is interpreted in the affected community. In this case, however, PITAC's Health and Information Technology Subcommittee has heard clearly that the unintended consequences of legislation are a direct impediment to maximizing the public benefit of NITRD-supported research and development. The recent publication of an interim final rule[23] by the Centers for Medicare and Medicaid Services (CMS) softens the Medicare stand on this issue, and this must be taken into consideration with all other applicable laws, regulations, and policies in the activity proposed.

4. Leveraging Federal Health IT Investments

Finding:

Federal health care entities have achieved significant performance and productivity benefits through major investments in EHRs, Computerized Physician Order Entry (CPOE), computer-aided Clinical Decision Support (CDS), health information interchange, and related technologies. Even within the most broadly implemented Federal health IT system (that of the VA), current rigorous data standards are lacking. This lack of standardization means that patient data stored in one region can be viewed and understood by humans in another region, but frequently will not be interoperable (i.e., computable) across health information systems. Only when standardized and normalized can the data be used to implement computer-aided clinical decision support.

There is some question as to whether freely sharing the software code for such systems would be valuable to the private sector. At a minimum, the design decisions that make such systems successful in terms of functionality, workflow support, decision-support protocols, and data definitions would be useful input into the national standard setting process. Some value may also be derived from looking at the private sector, where there are a few organizations and companies that assist in the deployment of public domain versions of the VA's EHR software called the Veteran's Information Systems Technology Architecture (VistA).[24]

Recommendation:

Develop a single set of standards for EHR systems that can be implemented across all Federally implemented EHRs and shared with the private sector. Develop pathfinder demonstrations that share appropriate Federal health IT implementation knowledge across all

---

[23] Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships (Phase II), *Federal Register*, Vol. 69, No. 59, Friday, March 26, 2004. Available at http://www.cms.hhs.gov/providerupdate/regs/cms1810ifc.pdf

[24] For example, WorldVistA at http://worldvista.sourceforge.net/ and Hardhats at http://www.hardhats.org/.

departments of the Government and with the private sector. Such demonstrations should use the standards analyses and recommendations of the Consolidated Health Informatics (CHI) eGovernment initiative as a starting place. At the appropriate level of development, demonstrations should target rural and disadvantaged communities that are underserved by private-sector vendors of health IT solutions. The new HHS position of National Health Information Technology Coordinator would be a logical leader to coordinate these efforts, which should be undertaken at the earliest possible opportunity.

Discussion:

There is clear evidence that investments by the Department of Defense (DoD), the Veterans' Health Administration (VHA), and the Indian Health Service (IHS) in their own health delivery services have significantly reduced preventable medical errors and increased provider productivity. The health care of more than 35 million people is currently recorded through these systems. This number far exceeds the population of people covered by all private-sector health IT systems combined. The cumulative Federal investment in health IT research, development, and deployment exceeds that of nearly all private-sector institutions. Clinical IT solutions have already contributed to DoD and VHA outcomes exceeding best-practice private-sector benchmarks for some chronic illnesses. Increased sharing of best-practice caregiver IT technology and standards across Federal agencies and the private sector could save considerable taxpayer resources.

Despite the clear value of these investments, the standards under which data are recorded vary from one site of care to another. These data standards include such aspects as data format, labels (standard data element names), terminology (standard name for a specific medical concept), codes (standard code for the same concept), limits, units, components, and criteria for situations in which a data element is to be recorded. Only systems that can produce normalized data that meet all of these standards are truly interoperable. Lack of agreement on these standards prevents the sharing of interoperable data (e.g., graphic depiction of blood pressure over time) and can limit data exchange to simple viewing of text. Because compatible messaging standards are being implemented across Federal electronic health systems, this sharing of normalized data is readily achievable if implementations are standardized at the data element level. Working with the private sector to set the standards and test their implementation in Federal health IT implementations will do much to move the whole industry forward.

5. Implementing a Standard Clinical Vocabulary

Finding:

Standardized clinical vocabulary is essential to computerized decision-support tools using sharable protocols that lower error rates and improve the quality of health care. Medical language must be recorded in standard ways so its meaning can be shared with other EHR systems in a manner that is interoperable and computable (i.e., able to be manipulated and combined with other data by a computer). This language must be coded in a standard manner, even if the concepts are referred to by different local names, displayed in different local languages, or depicted in different local alphabets. This requires the availability of a core set of standard clinical vocabulary terms that can be incorporated into EHR systems at every level to describe clinical concepts including problems, diagnoses, test results, and procedures. The

classification systems historically used to code medical diagnoses and procedures for reimbursement and population statistics are not adequate for these purposes.

In most medical practices today, a clinical encounter is recorded in the form of a detailed textual description (handwritten, typewritten, or transcribed from dictation) in the medical record. Most providers must then summarize this information by selecting entries from classification systems, such as ICD-9-CM[25] and CPT®[26], before submitting the clinical encounter for reimbursement. The coding process is often onerous and usually performed manually by the provider or a professional coder hired to scour the written record and find the codes for the classes that most closely fit the findings and events described in the record. Because of the reimbursement focus in coding, the selection of codes is frequently influenced by reimbursement implications, which may at times be in conflict with underlying clinical constructs.

There are significant barriers to overcome before standard clinical vocabulary can be widely implemented. Although easily expressed in medical terms in the text, standardized vocabularies have historically been very difficult for providers to implement in a manual charting environment. With the advent of EHR and CPOE systems, computer solutions can ease the challenge of recording standard codes for detailed clinical concepts.

HHS has adopted the Systematized Nomenclature of Medicine, Clinical Terms (SNOMED-CT)[27] as a standard medical vocabulary and purchased a license that allows all U.S. Federal and private-sector parties to use SNOMED-CT at no cost. HHS has also adopted the Laboratory Logical Observation Identifier name Codes® (LOINC®) vocabulary to standardize clinical laboratory results as another part of the core set. However, much research and support infrastructure work needs to be done, as well as realignment of financial incentives, before broad implementation can become a reality.

Recommendation:

Federal incentives are needed to enable the incorporation of SNOMED-CT into EHR systems so that those systems can exchange normalized expressions of clinical concepts, implement standard computer-aided decision-support protocols to reduce medical errors and provide more detailed information for quality-improvement programs. SNOMED-CT also must be freely available as part of a core set of standardized clinical vocabulary and supported as a continually improving standard that is kept up to date. Standard, automated mapping of SNOMED-CT to the International Classification of Diseases, Tenth Revision, Clinical

---

[25] The International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) is the official system of assigning codes to diagnoses and procedures associated with hospital utilization in the United States. Further information is available at http://www.cdc.gov/nchs/about/otheract/icd9/abticd9.htm

[26] CPT® is a trademark of the American Medical Association. The Current Procedural Terminology (CPT) is a copyrighted product of the American Medical Association (AMA), which must be licensed for use and is required to describe procedures performed in outpatient claims for reimbursement by most health benefit programs, including Medicare. Further information is available at http://www.ama-assn.org/ama/pub/category/3676.html

[27] SNOMED-CT is a dynamic, scientifically validated clinical health care terminology and infrastructure that provides a common language that enables a consistent way of capturing, sharing and aggregating health data across specialties and sites of care. More information is available at http://www.snomed.org/snomedct/index.html

Modification (ICD-10-CM)[28] must also be freely available. Financial incentives must be provided for EHR systems to generate SNOMED-CT coded clinical information (in Federal pay-for-performance programs, for example). A migration strategy must be adopted for Federal health program reimbursements to be based on the reporting of diagnoses and procedures coded in SNOMED-CT for clinical purposes. In the proposed rulemaking process of replacing ICD-9-CM with ICD-10-CM, HHS must avoid the potential for that migration to retard the adoption and implementation of SNOMED-CT in EHR systems. Study of alternative approaches may be required.

Each of these incentives must be researched, developed, and supported in the long term to assure successful implementation. The National Library of Medicine (NLM), the National Center for Health Statistics (NCHS), and the Centers for Medicare and Medicaid Services (CMS) as cooperating agencies of HHS should undertake this work that should also be coordinated with all other Federal agencies with health care interests. AHRQ should be involved in funding demonstration projects to gather objective feedback into the process.

Discussion:

The National Committee on Vital and Health Statistics (NCVHS) has already recommended that HHS transition quickly from requiring the ICD-9-CM classification system in HIPAA standard transactions to the new ICD-10-CM system. When HHS issues the regulations to implement that recommendation, it must be particularly careful to avoid unintended consequences, including a potential delay in the adoption of SNOMED-CT in EHR systems. HHS should make clear that such a delay would be very harmful and should provide a well thought out and supported migration strategy to encourage and support SNOMED-CT adoption.[29] The first step has already been taken; the HHS license for SNOMED-CT enables all Federal and private designers of EHR systems to freely incorporate this vocabulary and coding system. Significant controversy still exists, among caregivers, medical records professionals, and payers about the desirability of expending time and resources on implementing ICD-10-CM in a paper-based environment, rather than focusing on a rapid transition to an EHR environment implementing SNOMED-CT.[30] [31] [32]

---

[28] ICD-10 is used to code and classify mortality data from death certificates, having replaced ICD-9 for this purpose as of January 1, 1999. ICD-10-CM is planned as the replacement for ICD-9-CM, volumes 1 and 2. More information is available at http://www.cdc.gov/nchs/about/otheract/icd9/abticd10.htm

[29] NCVHS has recommended to HHS that they propose the move to ICD-10-CM based on a Rand study it commissioned. A contemporary Blue Cross Blue Shield Association (BCBSA) sponsored study done by the Robert E. Nolan Company concludes that "the vast majority of benefits asserted by proponents cannot be achieved by a conversion to ICD-10-CM or ICD-10-PCS without first implementing a standard clinical vocabulary." The concept of using a more refined/granular vocabulary system for reporting in the same terms used to record clinical concepts and events in the medical record was not included in these works, although the NCVHS recommendation raises the question of unintended consequences. See the NCVHS recommendations at http://ncvhs.hhs.gov/031105lt.htm , the Rand report at http://www.rand.org/publications/TR/TR132/ , and the BCBSA sponsored study at http://bcbshealthissues.com/relatives/20884.pdf

[30] Comments from AHIMA posted on PITAC website at http://www.itrd.gov/PITAC/

[31] Comments from HIMSS posted on PITAC website at http://www.itrd.gov/PITAC/

[32] Comments from BCBSA posted on PITAC website at http://www.itrd.gov/PITAC/

Since ICD-10-CM is a medical concept classification system that is more current than ICD-9-CM, the Federal government must also undertake the necessary research to create and support automated mapping from SNOMED-CT terms into ICD-10-CM. This would enable all providers, payers, and public health organizations to aggregate the clinical data from EHR systems that use SNOMED-CT in ways appropriate to the many uses for the aggregated information in low-cost, reliable, and comparable formats. It also provides a transition strategy for those who can only accept ICD-10-CM codes until they are capable of handling the full clinical details available in SNOMED-CT. This approach would also eliminate much of the labor-intensive administrative billing and reporting processes for providers.

6. Standardized, Interoperable EHRs

Finding:

Notwithstanding the value of exchanging existing sources of patient information, EHRs that are based on a common information architecture with highly standardized data definitions enable computer-aided decision support, automated medical-error detection, and rapid patient-population analyses for medical research, public health, and homeland security, and thus could have enormous national value. There is currently no data-level standard for the storage and retrieval of clinical information within EHRs. Most standards organizations, including Health Level Seven (HL7)[33], have emphasized the structure of the messages being exchanged between systems and have allowed significant variation in the content and internal organization of data within that structure.[34]

This lack of standardization, particularly of quantitative data, hinders interoperable use and requires a great deal of work on translations from internal representations to those representations that can be transmitted to and understood by another EHR system. Even within a single proprietary EHR product line, each instantiation of the product is apt to use different data layouts, largely dictated by the installation site. Recently adopted standards for pharmacy data, laboratory data, and radiological images are a step in the right direction but only a partial solution to this problem. Currently, there is little possibility for moving quantitative patient data across sites of care in a fully interoperable manner. There is a long and successful history of Federal leadership, primarily from NIH, in developing universally adopted nomenclature for disease staging, because of the need for such nomenclature in clinical research. Similarly, this is an area where Federal leadership can be used to encourage private-sector organizations to agree on data standards.

---

[33] HL7 is an American National Standards Institute (ANSI) accredited standards-developing organization that provides standards for the exchange, management, and integration of data that support clinical patient care and the management, delivery, and evaluation of health care services. More information is available at http://www.hl7.org/about/

[34] For example, HL7 does not specify whether blood pressure should be stored as one field of six digits or two fields of three digits. In fact, HL7 says nothing about how to represent blood pressure in an implementation, but only specifies a way to share this 'mini-battery' of test results with other applications.

Recommendations:

Develop a single set of data standards for the most common forms of clinical information. This effort should leverage efforts underway within Federally implemented systems (see Recommendation #3). Examples of data to be included in the standard are vital signs, examination findings, and review of systems information. These standards should be developed in the public domain in conjunction with voluntary standards-developing organizations such as HL7 and ASTM so that they may be implemented in proprietary EHR systems and also used as a fully interoperable transport standard between EHR systems. Coordination is needed across relevant HHS, VA, and DoD agencies, along with NIST, NSF, and others, with the leadership of the new HHS position of National Health Information Technology Coordinator.

Conduct research and development into low-cost tools for standardizing new and legacy digital data without disrupting current clinical workflow. Such tools might draw upon existing Federal projects for rules-based and statistically based natural-language processing and related technologies.

In addition to specifying the data elements and architecture, standards developed in this environment should also address the redundancy and persistence of core EHR data that are needed to create a reliable, federated health information infrastructure.

Discussion:

Although normalized clinical data standards have been advocated for decades and vendors of health IT systems generally assert adherence to standards, most current standards lack the specificity required for true interoperability. Even some vertically integrated systems of care using a single computing platform map data with sufficient variability in names and formats to impede interoperability and quantitative assessment. Moreover, fear of rapid obsolescence often impedes investment in present weak standards that lack probable longevity. One of the factors slowing the innovative development of full standards has been lack of funds and encouragement for leading-edge, private caregiver organizations. Federally funded regional pathfinder demonstrations that include significant sustained support for open, normalized EHR standards development are almost certainly necessary to accelerate progress in this area.

7. The Human-Machine Interface and EHRs

Finding

While the keyboard and mouse remain the predominant means for entering caregiver-generated information into EHRs, other methods hold considerable promise for improved performance. Although progress has been made with automated speech/text conversion, bar-code technology for medication administration, and direct transfer of digital information from diagnostic instruments, additional innovative solutions and improvements are needed to facilitate the entry of caregiver-generated data in a manner that saves personnel time and is minimally intrusive to the human relationship with the patient, while producing normalized data that can be used to support research, clinical decision support, and other automated improvements in health care.

Recommendation

Conduct research and development in innovative and efficient human-machine interfaces that are optimized for use in the health care sector. Research on the use of IT to improve the workflow for health care delivery functions is a particularly inviting target. Technology examples include:

- Improved medical-domain voice-recognition data conversion systems
- Improved automated entry of instrument data
- Improved templates that simplify and accelerate data entry without training
- Automated methods for converting both new and legacy electronic data to normalized form

Agencies involved in human-computer interface and data management research include relevant agencies in HHS and DoD, as well as NIST and NSF.

Discussion

Numerous caregivers have testified that pen and paper remain the simplest, most time-efficient method for data capture, far exceeding the efficiency of mouse and keyboard interfaces available today. Many acknowledge that the cost of the additional time spent on electronic data entry is more than recaptured as benefits downstream when data are recalled, displayed graphically, and linked to decision support. However, the benefits associated with the use of such health information technology are not often directly felt by those who must enter the primary data.

Aside from the time investment demanded by current human-machine interfaces, the effect of those interfaces on the human element of caregiver-patient contact must be considered. Typical screen and keyboard implementations are slower than dictation and may require the caregiver to turn away from the patient in order to record information, an act that can be objectionable to both. Many physicians are extremely facile in using dictation during or after the patient encounter to record critical information. Development of technologies that support the use of voice and other methods of data input that do not detract from patient interactions are preferable to forced retraining of physicians in the use of keyboards.

Technologies that should be considered for study include voice-recognition technology, use of slate computers and handwriting recognition, and other innovative human-machine interface technologies. Improved EHR data entry and recall technology and demonstrations of successful technology/protocol combinations will lower current barriers to the implementation of EHR at the point of care and greatly facilitate the realization of savings in quality and cost that are promised by this technology. Agencies involved in human-computer interface and data management research include relevant agencies in HHS (particularly NIH) and DoD (particularly the Defense Advanced Research Projects Agency [DARPA]), as well as NIST and NSF.

8. Coordination of Federal NHII Development and Implementation

Finding:

The PITAC previously recommended that a senior appointee in the Department of Health and Human Services coordinate all health information technology initiatives.[35] However, the bulk of development and deployment to date has been driven by the Departments of Commerce, Defense, Homeland Security, and Veterans Affairs, and coordination is necessary across all Federal health delivery and health-quality improvement systems. There is no evident mechanism for coordinating Federal NHII and EHR developments and implementations across the many departments involved. This is doubly important for privacy and security policy issues that cut across many Federal agencies and are central to the establishment and healthy growth of the NHII.

Recommendation:

Establish a senior body to coordinate the development and deployment of Health IT solutions across all Federal departments and agencies and to coordinate the associated technology transfer to and from the private sector. This body might be composed of a core group of individuals at the undersecretary level from each affected department and agency, with additional expertise acquired as needed. Federal policy recommendations relevant to the privacy and security issues that could impede the implementation of health IT should be an early product of this body.

Discussion:

The same EHR systems critical for improving patient care can also help accelerate clinical research and its impact on practice and improve pharmaceutical safety (pharmacovigilance) and biosurveillance for public health and homeland defense. Without broad senior-level coordination, there is strong potential for overlap or loss of collaborative opportunities through lack of awareness. In particular, senior leadership could help identify opportunities for dual use of EHR systems that could reduce total system costs. Coordination of Federal funding and participation in EHR standards-development organizations would assure that the results effectively serve the purposes of all involved Federal agencies and the private sector.

Health programs pervade most departments in the executive branch and routinely pose security and privacy issues that are best handled in a standard way. HIPAA provides a legal framework for managing security and privacy issues but does not provide specific protocols and security architectures. Currently, there is little coordination concerning health privacy and security within the Federal health sector and even less coordination with the private sector. Without some inclusive high-level locus for addressing this issue within the health sector, achieving NHII goals and efficiencies will be difficult because private communications and records are so central to the NHII vision. Moreover, the tight coupling between privacy/security and other aspects of the NHII require that addressing these issues be incorporated in the charter

[35] Recommendation 6, Report to the President on "Transforming Health Care Through Information Technology," President's Information Technology Advisory Committee, February 9, 2001. http://www.nitrd.gov/pubs/pitac/pitac-hc-9feb01.pdf

for any high-level Federal coordination body, such as the one recommended here. (See specific issues discussed in Part II.)

Part II – Promoting Secure, Private, Interoperable Health Information Exchange

9. Unambiguous Patient Identification

Finding:

Unambiguously identifying patients and linking their information from multiple sources is a major challenge both within and across clinical enterprises. Unless caregivers are able to access linked information on a given patient across the continuum of care, proper and cost-effective care cannot be rendered. Similarly, the ability to link patient data in an anonymous and secure fashion is critical to the national research enterprise, public health surveillance, and bio-preparedness.

Recommendation:

Convene an interagency, public/private task force to determine ethical, legal, and practical means for unambiguously identifying and linking patient data from multiple sources in a unique, secure, and trusted manner that protects patient privacy and gives the patient control over the use of his or her medical information. Activities of the task force should include an estimate of the costs and benefits associated with unique patient identifiers (IDs) derived from existing or novel patient attributes. The task force should consider existing models and ongoing private-sector efforts that emphasize private, rather than government, control of data storage, transmission, and sharing. There must be ongoing recognition of and accommodation for those people who wish to receive all or part of their care anonymously, as well as for those who are visitors to or temporary residents of the United States.

Discussion:

Caregivers consistently cite frustrations in assuring that EHR data actually apply to the patient before them; errors can be dangerous or even fatal. This limitation has surfaced as a major impediment in current communitywide data interchange projects. The problem is severe because a surprising fraction of all presenting patients have ambiguous identification or lack stable addresses or distinguishing names. The challenge is compounded by the scale of the region and population served and the number of care sites accessible to that population. Although the use of social security numbers for patient identification is advocated by some, there are numerous legal barriers to this and such use of SSN is opposed by significant constituencies. Representative procedures for assigning unique IDs include Universal Resource Names (URN) and Object Identifiers (OID). Existing policies against unique nationwide identifiers can be accommodated via technological means, but Federal support of ID technology development and demonstrations in a health context are essential to progress. Examples of technologies that might be explored include the following:

- Six-digit compression of the patient's social security number
- Biometric technologies

- Personal smart ID cards (e.g., cards displaying or communicating time-dependent passwords)
- Characterization of speech or handwriting
- Authentication means for anonymous entities.[36]

The President's Bioethics Council should be considered for leadership of this task with technical input from the Departments of HHS, Justice, and Defense, the VA, and NIST. Private-sector representation should include caregivers, institutions, and consumers.

10. Public Key Encrypted Internet Communications

Finding:

Encryption currently protects much national security and commercial information transmitted across the Internet. Despite permissive language in the security rules implementing the HIPAA[37] related to this use of the Internet, current CMS policies[38] require the use of hub and spoke architectures that generally use 1970s protocols such as Xmodem and Kermit.[39] This impedes the development of our National Health Information Infrastructure (NHII) by forcing use of expensive, largely obsolete communication links in lieu of securely encrypted, inexpensive Internet transactions.

Recommendation:

There should be no Federal impediment to Internet transmission of health data protected by secure cryptographic systems. Assuring the trustworthiness of such ciphers requires continued research and development on current and novel cryptographic algorithms, means for defeating them, and pathfinder demonstrations in health-relevant contexts. Agencies currently conducting such research include the National Security Agency (NSA), NIST, and NSF. CMS should be kept apprised of these research findings or participate in the research. A specific example would be to re-examine the current Medicare policy that prevents CMS contractors from using secure transmissions over the Internet. In the absence of a single coordinating body for certificate

---

[36] An example of anonymous authentication methods is Shibboleth, which is being developed by a university consortium: S. Cantor and M. Erdos, Shibboleth Architecture DRAFT v05 http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html

[37] The Administrative Simplification Subtitle of HIPAA and its implementing final security rule specify a series of administrative, technical, and physical safeguards for health plans, health care clearinghouses, and health care providers to use to assure the security of electronic protected health information. More information is available at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

[38] Current CMS Internet Security Policy issued on November 24, 1998, permits the use of the Internet "… as long as an acceptable method of encryption is utilized …" and lays out what those acceptable methods are in a reasonable way. However, the current CMS Business Partners Systems Security Manual dated March 28, 2003, instructs all business partners that "health care transactions (claims, remittances, etc.) are prohibited between Medicare carriers/intermediaries and providers over the Internet. This Internet prohibition also applies to using the Internet to transport CMS Privacy Act-protected data between carriers/intermediaries and any other party. See the CMS Internet Security Policy for a definition of protected data www.cms.hhs.gov/it/security ."

[39] Kermit and Xmodem are file transfer protocols that provide the means of transferring data between computer systems in an error-free manner. A comparison is available at http://www.sbsw.com/Articles/kermxmod.htm

authorities[40], bilateral encryption agreements across all health information systems may be needed. With the number of health entities that must communicate, this situation would be untenable. Therefore, timely studies should be commissioned to assess the current maturity and efficiency of encryption techniques and digital signatures for sharing health information and the efficacy of federalizing such techniques. It is particularly important to remove any regulatory impediments to e-mail communication between willing patients and their caregivers.

Discussion

Public Key PK ciphers[41] have made Internet encryption practical by permitting anyone to send encrypted messages to anyone else using the recipient's publicly posted key. These PK ciphers commonly convey secondary symmetric keys to other ciphers that protect the body of each message. Several algorithms exist, such as prime-number and elliptic-curve methods for PK; Data Encryption Standard (DES), Triple DES, and the Advanced Encryption Standard (AES) for symmetric key; and Digital Signature Algorithm (DSA) for digital signatures. New methods for breaking these codes are constantly sought to ensure that the ciphers are robust. The success of these algorithms is evident in their widespread use for transmission of much national security data across the Internet, and vendors could provide similar capabilities to the health sector at costs well below those for currently mandated methods. It is essential that Federal actions to ensure cryptographic security and practicality substantially outrun efforts by others to compromise them inappropriately. Recently approved specifications such as the Security Assertion Markup Language (SAML) and Web Services Security (WSS) additionally support the security requirements for multi-party scenarios where intermediate nodes might otherwise decipher messages traversing consecutive point-to-point links.[42] While the above recommendation focuses on protecting information in transit, that same information must naturally be protected "at rest." Medical records need to be protected from tampering, inappropriate access, and accidental disclosure by current industrial methods that include strong authentication, authorization, and encryption. Particularly critical are security measures applied to administrative systems.

11. Trust Hierarchy and Authentication

Finding:

Health information can only be accessed with adequate security and privacy if there are clear means for verifying the identities of those accessing and altering data. The lack of defined

---

[40] Also see Recommendation 11 concerning trust hierarchies, and Recommendation 8 concerning policy issues and Federal coordination.

[41] PK encryption is a cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message. The public and private keys are related in such a way that only the public key can be used to encrypt messages; only the corresponding private key can be used to decrypt them; and it is virtually impossible to deduce the private key if you know the public key. Because PK codes are computationally quite slow, they normally only convey keys to the much faster codes that protect the body of each message. An introduction can be found at: http://www.krellinst.org/UCES/archive/modules/charlie/pke/

[42] For SAML see http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, and for WSS see http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

standards for security and the lack of an accepted hierarchy of trusted authentication agents impede the development of the NHII and associated cost-effective data communication systems.

Recommendations:

The Federal government, through NIST in the Department of Commerce or another civil, cross-department technology entity, should accelerate the definition and establishment of extensible, hierarchical authentication trust trees and standards for optional use by the private health sector, where these trees include both government and private providers; supportive research and development are required.

Additional research should address how the current legal framework for authenticating written signatures (notary public laws) might be extended to electronic signatures as part of this trust hierarchy. Supportive research and development are required from agencies such as NSA, NIST, NSF, DoD, and the General Services Administration (GSA).

Discussion

Trust requires robust standards for authentication and authorization. Is an individual or other entity actually who or what it says it is, and precisely what standards were employed to establish that identity or authorization? Traditional face-to-face authentication and limited circulation of paper records within single practices are rapidly becoming obsolete security measures in our emerging, multi-caregiver electronic environment. Today there is a lack of defined standards for electronic authentication and for communicating authentication and authorization instantly to users. The problem has both procedural and technical elements. Technical methods are required for transmitting or securing almost instantaneous authorizations and authentications via the Internet in a robust manner, and the development and demonstration of such methods for health care are recommended. One recently demonstrated approach employs tiny encrypted “proofs” that link individuals or entities with authorizations and authentications that are widely replicated across the network by the trusted authentication agent in order to eliminate single-point failures of inquiries or possible congestion and delay. Similar proofs can establish instant trust in that same agent via a tree linking that agent to Federal or other trusted agents. For example, a payer might validate a physician’s invoice by using such proofs to ensure that the physician has a valid ID and is currently board-licensed, and that the board is recognized by the American Medical Association. Such trust trees can be automatically traversed back to widely trusted nodes in seconds.

A representative procedural challenge involves definition and implementation of robust object identifiers that precisely define the process used to authenticate identities and authorizations. For example, one widely used method sends passwords to the listed e-mail address of an inquirer. If such a step were one part of a sequential authentication or authorization process, how should this sequence be represented? An authentication chain is only as strong as its weakest link. Recommendation 9 concerning unambiguous patient identification is also relevant to caregiver authentication technologies.

12. Tracing Access Requests

Finding:

Enabling patients, physicians, and hospitals to identify those who access patient information and the appropriateness of their access helps deter patient privacy violations. Experience to date

suggests that it is nearly impossible to determine in advance which caregivers will have a legitimate need to access the information of a given patient. Systems that attempt to limit access only to a defined group of caregivers for a given patient have been found to hinder the care process. A more effective approach has been that of access tracking.

Recommendation:

Federal policies should promote development and use of data-access tracking (or auditing) systems in the health care sector, including research and development of such means and pathfinder demonstrations in large systems.

Discussion

Only systems that routinely and securely record such access and that simplify review of that access can support the level of privacy required by HIPAA. Most legacy health information systems are capable of tracking changes additions, deletions, and updates — to a database. However, many times these "audit trails" are turned off or kept on only for the most sensitive records because of the computational and storage resources they consume, or they are configured only for transaction backup purposes. In addition, most are not configured to record accesses or "reads" to the data at all. In any case, few systems have the automated tools available to make it practical to analyze the large amounts of data that would be produced by such monitoring, so analysis is typically done manually and is extremely limited. Research, development, and demonstration of cost-effective access-logging and analysis systems are critical to support privacy protection of patient data.

Current evidence shows that knowing that access is being tracked and that disciplinary action will result from infractions of access policy has been helpful in maintaining patient privacy. Serious violations can be reduced further by additional clear warnings at the moment of possible transgression, a so-called "break the glass" access barrier that requires users to justify their need to make the access. These warnings must be muted during access by the primary-care physician and certain others. They are not effective if they occur during normal business operations, but it is not easy to determine when an access is out-of-the-ordinary in the complex world of health care, where roles, locations, and tasks are relatively unpredictable. Research, development, and demonstration of such warning systems in diverse caregiver environments are required to help deter electronic privacy violations nationally.

APPENDIX I. PITAC HEALTH AND INFORMATION TECHNOLOGY SUBCOMMITTEE FACT-FINDING PROCESS

In addition to their own professional experiences and in-depth knowledge of the literature in the field of health care and information technology, the members of the PITAC Health and Information Technology (HIT) Subcommittee obtained information for this report from several othersources:

- November 12, 2003, PITAC meeting
- January 8, 2004, HIT Subcommittee meeting
- January 12, 2004, site visits
- February 25, 2004, Town Hall meeting at the Health Information Management Systems Society Conference
- Additional public oral and written statements that resulted from the above activities

These activities are described below in further detail.

November 12, 2003, PITAC Meeting

At this public meeting held via WebEx and in person in Arlington, Virginia, formal presentations by seven invited experts were given in the following order:

- ***Elias Zerhouni, M.D., Ph.D., Director, National Institutes of Health (NIH)***
- ***Mark B. McClellan, M.D., Ph.D., Commissioner, Food and Drug Administration (FDA)***
- ***Anthony Principi, Secretary, and Jonathan Perlin, M.D., Ph.D. Deputy Undersecretary for Health, Department of Veterans Affairs (VA)***
- ***Kevin Kiley, M.D., Director, Walter Reed Army Medical Center***
- ***Carolyn Clancy, M.D., Director, Agency for Healthcare Research and Quality (AHRQ)***
- ***David Kibbe, M.D., M.B.A., Director, Center for Health Information Technology, American Academy of Family Physicians (AAFP)***
- ***David B. Nelson, Ph.D., Director, National Coordination Office for Information Technology Research and Development (NCO/ITR&D)***

Speakers were asked to describe the activities of their organization in health and information technology and to respond to four questions:

- What do you imagine could be achieved in the next few years by aggressive deployment of today's technology?
- What are the barriers to this?
- What steps should be taken to surmount these barriers?
- What do you imagine could be achieved in ten years with appropriate research and development investments in the area of health and information technology?

Each presentation was followed by questions by PITAC members. (To view or hear these presentations or to read meeting minutes, please access http://www.itrd.gov/pitac/meetings/2003/index.html.)

January 8, 2004, Health and Information Technology Subcommittee Meeting

On January 8, 2004, in Washington, D.C., the Health and Information Technology Subcommittee invited national experts to inform the members about two critical issues:

- Health information exchange architecture. The subcommittee members examined existing architectures for health information interchange to determine if one or more systems that could exchange data from one site to another were sufficiently mature to recommend as a standard for the NHII.
- Security and privacy of health information. Misunderstanding about HIPAA has imposed limitations on security and privacy that are slowing adoption of health information exchange. The experts were asked to address computer security and appropriate protocols.

The following experts addressed these questions:

- ***J. Marc Overhage, M.D., Ph.D., Associate Professor of Medicine, Indiana University School of Medicine and Investigator, Regenstrief Institute for Health Care***
- ***Joseph Casper, Executive Vice President and Managing Director of Technology, First Consulting Group and Patient Safety Institute (PSI)***
- ***John D. Halamka, M.D., M.S., Chairman, New England Health Electronic Data Interchange Network (NEHEN) and Chief Information Officer, CareGroup Health System and Harvard Medical School***
- ***Nick Augustinos, M.B.A., Vice President, Care Data Exchange, Quovadx***
- ***Peter Szolovits, Ph.D., Professor of Computer Science and Engineering, MIT***
- ***Betsy Appleby, Program Manager for the Department of Defense Public Key Enabling, Defense Information Systems Agency (DISA)***

- ***David Temoshok, Director, Identity Policy/Management, Office of Governmentwide Policy, General Services Administration (GSA)***

Site visits

On January 12, 2004, subcommittee members visited Swedish Hospital and Peace Health in Seattle, Washington, where demonstrations by the Patient Safety Institute (PSI) on capturing health data from legacy systems were conducted. The PSI implementation is a "viewer" that tracks the location of patient records and reports data in a "non-standardized" form.

Members then visited Puget Sound Veterans Administration Hospital to view the VA's Clinical Patient Record System, which can bring up images, including radiology and ultrasound, at the bedside.

Town Hall Meeting

At a Town Hall meeting held during the Health Information Management Systems Society (HIMSS) meeting attended by about 80 people in Orlando, Florida, in February 2004, the HIT Subcommittee heard from 23 speakers offering a broad spectrum of perspectives on three questions:

1. What are the primary barriers to the implementation of health information technology in general, and specifically to electronic health records?
2. Where is the biggest return on investment for providers (including groups and clinics) and for consumers from investments in health IT?
3. What can the Federal government do in terms of information technology research and development to help overcome these barriers?

Public oral and written comments

Several individuals and organizations sent in comments on specific issues raised during the meetings held between November and February. These were also taken into account in the discussion, findings, and recommendations in this report.

(Formal written comments received will be listed and posted on a website.)

APPENDIX II: ACRONYMS

ACP	Advanced Cyberinfrastructure Program
AES	Advanced Encryption Standard
AHRQ	Agency for Healthcare Research and Quality
ASPE	Assistant Secretary for Planning and Evaluation
ASTM	American Society for Testing and Materials
BCBSA	Blue Cross Blue Shield Association
CBO	Congressional Budget Office
CCR	Continuity of Care Records
CDS	Clinical Decision Support
CEA	Council of Economic Advisors
CHI	Consolidated Health Informatics
CMS	Centers for Medicare and Medicaid Services
CPOE	Computerized Provider Order Entry
CPT	Current Procedural Technology
CRA	Computing Research Association
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOJ	Department of Justice
DSA	Digital Signature Algorithm
EHR	Electronic Health Record
FDA	Food and Drug Administration
GAO	General Accounting Office
GSA	General Services Administration
HHS	Department of Health and Human Services
HIMSS	Health Information Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HIT	Health and Information Technology
HL7	Health Level Seven
ICD-9-CM	International Classification of Diseases, Ninth Revision, Clinical Modification
IHS	Indian Health Services
IT	Information Technology
NCHS	National Center for Health Statistics
NCO	National Coordination Office
NCVHS	National Committee on Vital and Health Statistics
NEHEN	New England Health Electronic Data Interchange Network
NHII	National Health Information Infrastructure
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development

NLM	National Library of Medicine
NSA	National Security Agency
NSF	National Science Foundation
OGC	Office of the General Counsel
OID	Object Identifier
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PITAC	President's Information Technology Advisory Committee
PK	Public Key
PKI	Public Key Infrastructure
PSI	Patient Safety Institute
R&D	Research and Development
ROI	Return On Investment
SAML	Security Assertion Markup Language
SNOMED-CT	Systematized Nomenclature of Medicine, Clinical Terms
URN	Universal Resource Name
VA	Veteran's Administration
VHA	Veteran's Health Administration
VistA	Veteran’s Information Systems Technology Architecture
WSS	Web Services Security

ACKNOWLEDGEMENTS

This report is designed to share the findings and recommendations of the President's Information Technology Advisory Committee (PITAC) on health information technology with the President, the Administration, Congress, the broader health care delivery and information technology communities, and the general public. Many people contributed to the substantive content and design of this document over several months.

First, the PITAC co-chairs extend special thanks to the members of the Health and Information Technology Subcommittee – Jonathan Javitt, Peter Neupert, and David Staelin – who dedicated countless hours above and beyond their normal workload. Their contributions are reflective of their commitment, not only to this report, but also to the advancement of health care delivery and information technology in the United States.

The PITAC thanks the National Coordination Office for Information Technology Research and Development, particularly William Braithwaite, Sally Howe, Elizabeth Kirk, Martha Matzke, Virginia Moore, David Nelson, and Diane Theiss for their contributions to supporting and documenting meetings; drafting sections of the report; critiquing, editing, and proofreading the numerous drafts; and contributing to the substantive dialogue that led to this final report.

Finally, thanks also go to Nicole Ausherman of Noesis, Inc. for creating the document's design, structuring its layout, and overseeing the administration of its printing.