I dedicate this effort to the memory of Prof. Swamy Laxminarayan, a constant source of inspiration and wisdom to those many that cross his path...

I write these lines with mixed emotions. Our dearest friend Swamy is now with us only in spirit. I coedited past special issues of IEEE Engineering in Medicine and Biology Magazine with him, namely, “The New Face of Terrorism: Combating Bioterrorism with Biomedical Engineering” [1], a year after 9/11 (September/October 2002), and “Protecting the Homeland: The Many Facets of Homeland Security.” January/February 2004 [2]. Therefore, I would like to dedicate this body of work to his memory.

This special issue is also the last to be published under the guidance, and the tender love and care, of John Enderle, as the editor-in-chief of IEEE Engineering in Medicine and Biology Magazine. As an editor-in-chief, John Enderle provided an extraordinary service for the IEEE Engineering in Medicine and Biology Society (EMBS) and IEEE Engineering in Medicine and Biology Magazine. As the editorial remarks in the 2004 issue reflect: “Editor-in-Chief John Enderle’s foresight to keep our readers abreast of the current and upcoming developments and initiatives is a source of constant encouragement to the biomedical engineering community to take on a broader role in the continuing fight against terrorism.” I take this opportunity to thank John for all the years of strong and visionary leadership and for the wonderful opportunities that he provided to bring forward before the EMBS community broader, meaningful, and highly relevant scholarly perspectives, which attempted to tackle the tough and persistent problems so evident in the times in which we live.

Why Protection of the Health Care and Public Health Critical Infrastructure and Key Assets?


What will it take to focus our attention toward ensuring our health care and required levels of protections for our public health critical infrastructures and key assets?

The theme of this special publication focuses on a broad range of science and technology issues as well as the economical, political, and policy interplays within the health care and public health critical infrastructures and key asset areas. The scientific community and the EMBS recognize intimately that preparing for the provision of health care, and erecting our public health system of tomorrow, is not just a matter of converging heterogeneous technologies but of people and processes as well. In this respect, and fundamentally, this special issue will attempt to convey to readers that efforts are needed by all parties involved in areas for improving health care deliveries and the public health infrastructures, and critical aspects related to interoperability [3] and the interdependence of processes and systems should be at the forefront of all future considerations. This special issue will, therefore, be centered around the topic of uninteroperability.

Everything seems unrelated, and yet it is related.

Everything is connected, and yet, functionally, it is disconnected.

There is a need to use a systems approach and have a holistic view of the problem; to be able to see the whole and not just discrete pieces; and help determine, for example, unintended consequences, which are absent.

It is necessary to integrate multidisciplinary and interdisciplinary orientations and activities when trying to understand the problem and moving toward generating potential solutions; yet, present approaches are grossly insufficient in this respect.

The problems we routinely experience with respect to medical errors, such as adverse drug effects, occur and are perpetuated because of our silos or stovepipes of information.

Content-wise, topics covered include failures to ensure our national security strategy for water, the need for protection of imported foods, a view of the state of our local and state public health infrastructure, electromagnetic interference in a hospital, a novel method of using geographical information systems to fight hospital infections, vaccine registries, supply chain...
Our health care system is in serious trouble. Nearly 50 million Americans are uninsured. Health care costs exceed US$2 trillion a year and are soon expected to double. We spend almost 16% of our gross domestic product on health care, which is more than that of any other industrialized country and double the European Union average. More families go into bankruptcy because of health care expenses than for any other reason.

However, for all this money, we get a mediocre product. We have the best doctors, the best nurses, the best equipment, the best procedures, and the best medical education in the world, yet as many as 100,000 Americans are killed every year because of unnecessary and avoidable medical errors. Life expectancy, obesity rates, and infant mortality rates are embarrassing by most international measures. What’s wrong?

The fundamental problem in health care is market failure, with three core components. First, the American health care system does not optimize quality or invest in prevention, even where improved care would lower the cost. We know, for example, that when intensive care units consistently take certain preventative measures to curb hospital-acquired infections, patients spend less time in the hospital, and care is less expensive. However, quality regimes that keep patients healthier can create financial penalties for hospitals that are paid on a fee-for-service basis.

This brings us to the second problem, the health care payment structure, in general, which is at odds with the public interest. Today, providers are compensated based on the quantity of care they provide, rather than on whether that care conforms to the best practices or delivers the best outcomes. That doesn’t make sense, and it creates an environment that rewards cost-shifting instead of cost-saving.

Third, health care does not have the information technology infrastructure to support the improvements we need. Americans use technology every day, at our offices, in our homes, in our cars, and even in our pockets. We keep lists of phone numbers and appointments on computers and handheld devices; we book flights, purchase gifts, and manage our bank accounts using the Internet. Go to Amazon.com, and they remember what you’ve bought, and guess what you might like. And yet, when you last visited your doctor, chances are that your medical records were in a paper file, that you got a paper prescription for any medications you needed, and that you had to fill out that clipboard for the umpteenth time.

Last May, I introduced three bills to address these problems, including the National Health Information Technology and Privacy Advancement Act of 2007 (Section 1465). This bill would create a national, private, nonprofit corporation to plan, initiate, develop, finance, and manage our national health IT infrastructure.

Today, about 28% of American doctors store and manage their patients’ health records electronically. Fewer than 10% use electronic systems to issue prescriptions. Yet, a well-functioning, interoperable health IT system would result in enormous annual savings to the health care system (an estimated US$81–346 billion annually). It would help avoid medical errors, including adverse drug interactions. It would speed up the processing of insurance claims and the update of medical information, eliminating duplication and improving public health. We need to bring health care into the 21st century, and significantly improve the quality of care for millions of people in our country.

Because every American family needs and deserves high-quality, affordable health care, and because tackling the huge challenge of rising health care costs will make our country more prosperous and more secure, we need serious and far-reaching health care reform, and we need it now. However, for any such reform to succeed, we first have to fix the broken, administrative and bureaucratic machinery that now stands in the way of efficient and effective health care.

Properly repaired, our health care system will reduce costs, improve care, enhance innovation, and significantly improve the quality of life for millions of Americans. More important, it will move us a critical step closer to every American family getting health care they can afford. That makes the work of reform very much worth doing.
attention of the biomedical engineering community, people mostly think about protecting hospitals, outpatient clinics, emergency care, medical equipment. Only in the last few decades have IT, processes, people, and activities begun to be included as a part of that grouping as well. Recent technology moves have included the National Health Information Network (NHIN), telemedicine, electronic/patient health records (EHR/PHR) initiatives, computer decision support systems (CDSSs), patient management via the Internet, consumer informatics, home care, security of medical information, bioinformatics,

Special Comments

By Robert Kolodner, National Coordinator for Health IT
Charles Friedman, Deputy National Coordinator for Health IT, Department of Health and Human Services

We congratulate the authors of this excellent collection of articles examining important national and international imperatives for infrastructure and interoperability in pursuit of better health for all people. As many of the articles suggest, health information technology (IT) is one of these critical infrastructures. The Office of the National Coordinator for Health IT (ONC) serves as the custodians for the United States Government of a “national health IT agenda” that would develop and implement a nationwide, secure, interoperable health IT infrastructure.

The importance of a robust health IT infrastructure as a foundation for any significant health care reform has been recognized by a broad spectrum of health stakeholders and health policy experts. Moreover, to monitor and protect the health and security of communities, aggregated health information must link with a variety of other data sources that affect health, such as food, water, environmental, while respecting and protecting the privacy of individuals. The integrity of the health IT infrastructure is vital to the nation’s safety, especially in times of national emergencies. Fortunately, the need to advance the health IT has enjoyed and continues to enjoy bipartisan support.

ONC has worked with federal agencies to create the ONC-Coordinated Federal Health IT Strategic Plan that was released to the public on 3 June 2008. The plan has several features that align with the articles in this collection. The plan identifies two goals: enabling patient-focused health care and improving population health. Population health is specifically defined to include public health, biomedical research, quality initiatives, and emergency preparedness. In the plan, objectives are identified for each goal to address each of four themes: privacy and security, interoperability, IT adoption, and collaborative public-private governance. Attached to each of the resulting eight objectives are strategies to meet these objectives and specific actions to enable the strategies. The plan includes measures for each objective and milestones for each strategy to assess progress along the way.

The plan is intended to be a complete, structured expression of what will be required to achieve an interoperable health IT infrastructure for this nation, supporting all aspects of health. It also offers several messages that are relevant to this collection of articles and their common themes of infrastructure and interoperability. The plan stresses the absolute imperative of building a unified health IT infrastructure supporting personal health, health care, and the component activities of population health. The nation cannot afford to build and sustain separate infrastructures for these different pursuits, and the lack of a unified health IT infrastructure could prevent the necessary flow of data between response teams and public health agencies in times of emergency, between electronic health record systems in physician offices and public health agencies that can detect disease outbreaks, and between the provider and personal health records systems that can help individuals manage their own health.

Although we have much work ahead of us, the United States is making significant progress toward an infrastructure supporting the secure exchange of interoperable health information. Infrastructure and interoperability require standards for information representation and exchange. Efforts coordinated by ONC are leading to the creation of nationally harmonized and recognized standards. We have established a process that works in annual cycles. Each year, priority areas of health care and population health requiring standards are identified; existing standards are then harmonized, leading to a national recognition and incorporation into criteria for certification of health IT products.

Building on these standards, a cooperative involving public and private organizations across the country is working to test and refine the standards, technical specifications, and agreements necessary for the unified solution that we call the Nationwide Health Information Network (NHIN). The NHIN, running on the commodity Internet, is the health IT infrastructure component which allows the secure exchange of electronic health information among a variety of networks such as regional health information organizations, integrated health care delivery systems, organizations that support personally controlled health record, and federal agencies. Information exchange using the NHIN supports personal health, health care, and population health. The concept is simple and elegant: an entity using the specifications and abiding by all the agreements that comprise the NHIN can exchange information with any other compliant organization. On 23 September 2008, progress toward an NHIN was demonstrated by 18 organizations that exchanged health information with one another. This demonstration showed that the concept of the NHIN could work and illustrated the value having a unified infrastructure for health information exchange.

In this spirit, we encourage the readers of these articles to think nationally, and even globally, as they consider the importance of information infrastructure and interoperability. In addition to seeing each important contribution as a contribution in and of itself, the readers should consider these works as a set and envision what will be possible as we move toward a unified infrastructure embracing the spirit and intent of all of them.
privacy, etc. Because of the research and development funds that many members in our community may rely on, many will immediately associate the topic to the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), the Agency for Health Research and Quality (AHRQ), the Food and Drug Administration (FDA), the Health Resources and Services Administration (HRSA), and the Centers for Medicare & Medicaid Services (CMS). A few more may think about the Department of Energy (DOE), Department of Commerce, Department of Defense (DOD), Department of Agriculture (USDA), DHS, the Environmental Protection Agency (EPA), the Department of Interior’s U.S. Geological System (USGS), the National Aeronautics and Space Administration (NASA), the National Science Foundation, and the National Oceanic and Atmospheric Administration (NOAA).

Yet, George Mason University’s Critical Infrastructure Report (CIR) of August 2008 reported on the health care and public health sector. According to the authors, a summary of the health care and public health sector major elements incidentally includes the following: health care personnel, hospitals (including specialty hospitals), ambulatory facilities (including office practices and dental offices), long-term care facilities, home health agencies, pharmacies, health departments, health-related laboratories, pharmaceutical manufacturers, medical device and supply companies, blood products centers, health insurers, and other payers. All these facilities and assets involve lack of an effective plan could hamper response efforts. One key finding of the investigation was the need to improve our nation’s medical surge capacity, enabling us to provide adequate health care for tens of thousands of injured people. Options for providing that surge capacity include field hospitals for triaging patients and prepositioned medications, supplies, and equipment at large public facilities, such as convention centers or stadiums.

If such a disastrous attack should occur, a well-planned, vigorous, and effective response by federal agencies will be critical to augment the work of state and local governments and nonprofit and private-sector organizations. Because of the logistical issues associated with marshaling a significant federal response, however, local first responders must assume that the federal government will not be able to provide support for the first 24–72 h after a catastrophic disaster. Communities must account for this reality in their preparations.

The Department of Homeland Security’s Metropolitan Medical Response System grant program provides funds to help hospitals, fire departments, public health departments, and emergency medical services develop coordinated plans for responding to mass casualty events. The program was created in 1996 after the Oklahoma City bombing, and the Sarin gas attack in Tokyo illustrated the need for localities to be prepared for a mass-casualty attack. Last year, the grant program was funded at US$41 million. I recently introduced legislation with Chairman Lieberman to improve this program and ensure that a jurisdiction in every state has access to direct funding. Under the bill, grant recipients would be able to use funds to prepare for all hazards, whether from acts of terrorism, hurricanes, pandemic influenza, or other mass-care disasters. This will ensure that health and medical personnel in major population centers in every state are prepared to respond to catastrophes.

Our nation has made great progress in preparing for the health care needs associated with major disasters. Unfortunately, no disaster is the same, and our response will need to be flexible to meet the exigencies of the moment. As we develop strategies to meet these future challenges, we must ensure that funding and training for first responders and medical personnel keep pace with evolving threats. We must bolster communications and planning at all levels of government, with nongovernmental organizations, and the private sector. These steps will help save lives when catastrophe strikes.
the private sector and the public sector (private and public companies and federal, state, local, and tribal governments). Depending on whom you ask, and what the basis of their experiences are, the aforementioned represents some views; many others are either incomplete or completely off the mark.

Since 9/11, we have seen many instances where other parts of the health care or public health critical infrastructure and key assets have failed. Some diverse examples are listed.

- The contamination of the U.K. portion (Chiron) of the flu vaccines (about 46 million, October 2004) was a major crisis considering that every year, an average 36,000 Americans die from the common flu and that more than 200,000 are hospitalized.
- The state of our emergency departments (EDs) (June 2006) is another example. The Institute of Medicine (IOM) published three major reports regarding the state of our nation’s EDs. One of its findings was that many of the 41 million uninsured people use these facilities for regular care. “As a result, ambulances are turned away from EDs once every minute on average, and patients in many areas may wait hours or even days for a hospital bed. Moreover, the system is ill prepared to handle surges from disasters such as hurricanes, terrorist attacks, or disease outbreaks.” It is clear that in the case of a major emergency (e.g., pandemic flu), we have no capacity to address it.
- The contamination of Baxter’s heparin resulted in deaths of at least 80 persons (early 2008).
- “Lead contamination of drinking water became a major issue in Washington, District of Columbia, in 2004, when news reports revealed marked increases in the levels of lead in tap water. The local water authority’s failure to effectively inform the public about the high lead levels angered citizens and damaged public trust in the local water supply. These events led policy makers to examine the adequacy of the EPA’s lead in drinking water rule, including the rule’s monitoring and public notification requirements, and EPA and state enforcement of the rule. Oversight hearings were held on these issues during the 108th Congress, and legislation to strengthen lead regulation was offered but not enacted” [4].
- On 10 March 2008, an Associated Press investigation showed that a vast array of pharmaceuticals, including antibiotics, anticonvulsants, mood stabilizers, and sex hormones, has been found in the drinking water supplies of at least 41 million Americans.
- There are many cases of food contamination (e.g., salmonella, mad cow disease, ciguatera) from both local producers or suppliers and imported ones.
- According to the 26 July 2007 Office of the Inspector General Report (DHS) on the failure of the National Biosurveillance Integration System (NBIS), “Since 2001, an estimated US$32 billion has been spent on federal biosurveillance and biodefense IT programs (e.g., CDC’s BioSense, DHS’ BioWatch, FDA’s Carver and Shock). To date, there is no coordinated effort to correlate the data gathered into anything resembling intelligence, never mind injecting actual intelligence reports into the mix involving biosurveillance. In April 2004, HSPD-10 (biodefense for the 21st century) directed DHS to coordinate all disparate biosurveillance programs that appeared since 9/11, with the goal of creating a national bioawareness system that will detect a biological attack at the earliest possible moment and permit initiation of a robust response to prevent unnecessary loss of life, economic impact, and social disruption” [5].
- In May 2007, Mr. Andrew Speaker, an attorney from the United States, caused a major health scare in the United States and abroad when he flew to and from Europe while knowingly infected with a drug-resistant form of tuberculosis (TB). Although initially diagnosed with multidrug-resistant TB (MDR-TB), Mr. Speaker was subsequently confirmed to be infected with extensively drug-resistant TB (XDR-TB). When public health officials realized that he had left the United States to travel in Europe (Italy, Greece, France), they began working with other federal and state authorities, as well as international bodies (e.g., Canada’s border control), to limit the spread of the disease by denying him entrance to this country. Instead, he was never stopped anywhere so as to protect the public.
- As in the TB case where there was a complete lack of interoperability between the authorities in Italy, Greece, France, and Canada and the CDC and DHS, the same could be said about all the other failures. As mentioned at the beginning of this editorial, and paraphrasing, in all these instances:
  - everything that seemed connected was functionally disconnected
  - there was a need to use a systems approach and have a holistic view of the problem; to be able to see the whole and not just discrete pieces; and help determine, for example, unintended consequences, which are absent
  - it is necessary to integrate multidisciplinary and interdisciplinary orientations and activities when trying to understand the problem and moving toward generating potential solutions; yet, present approaches are grossly insufficient in this respect
  - the problems that we routinely experience are perpetuated because of our silos or stovepipes of information.

**Legislative and Policy Input**

This past September 11th, I had the opportunity to attend Capitol Hill “Steering Committee on Tele-Health and Healthcare Informatics” meetings organized by my colleague Neal Neuberger, President of Health Tech Strategies, LLC. During lunch, Senator Sheldon Whitehouse gave a terrific Keynote focused on the many problems affecting our current Health Care delivery System. After this presentation, I had the opportunity to speak with him, and he was very gracious to accept my invitation on behalf of the EMBS, to compose certain comments for this special issue of our magazine. In his comments, he has surfaced many important issues, including the lack of medical insurance coverage for almost 50 million Americans, the need to transform our system through functional interoperability to eliminate medical errors, improve quality, and decrease costs while protecting the security and privacy of this information, to name a few.

Drs Robert Kolodner and Charles Friedman, the National Coordinator (NC) for Health IT and his Deputy, respectively, were also very gracious to provide their comments that explain how their office (ONC) has worked with the federal agencies to create the “ONC-Coordinated Federal Health IT Strategic Plan,” which was released to the public on 3 June 2008. They also elaborate on their plans related to the National Health Information Network (NHIN) (a group of IEEE Medical Technology Policy Committee (MTPC))
Members led by Tom Jepsen created the IEEE-USA e-Book titled “Interoperability for the National Health Information Network”. Their message is clear on how the integrity of the health IT infrastructure is vital to the nation’s safety—especially in times of national emergencies.

Additionally, we are privileged to have comments from Senator Susan Collins in this issue. Senator Collins chose to provide comment on the Public Health critical infrastructures, and the need to improve the preparedness and response aspects during major catastrophes. Senator Collins is currently the ranking member and past chair of the Senate Homeland Security and Government Affairs Committee. She has traded places with Senator Joseph Lieberman (as chair and ranking member of this committee) and has worked with him on many issues. As a result of the committee’s investigation into the response to Hurricane Katrina and threats from nuclear terrorism, they introduced specific legislation in 2006. They also expanded the Metropolitan Medical Response System grant program, providing funds to assist hospitals, fire departments, public health departments, and emergency medical services to develop coordinated plans toward responding to mass casualty events.

On behalf of the EMBS, I would like to acknowledge the outstanding and timely contributions of these public servants, and applaud their continued efforts to improve our Health Care and Public Health Critical Infrastructures.

Acknowledgments
The views expressed in this editorial are those of the author and do not reflect the official policy or position of the National Defense University (NDU), the Department of Defense, or the U.S. Government.

The late Swamy Laxminarayan and I had the opportunity to coedit the previous two issues of IEEE Engineering in Medicine and Biology Magazine. Secretary T. Thompson, Senators Rockefeller, Frist, and Lieberman, and Former Speaker of the House Newt Gingrich provided our nation and our technical community with valuable inputs. Changing our current system from short-sighted islands of excellence (stovepipes) into one that is both cost and medically effective and efficient will require true interoperability among multidisciplines and interdisciplines where a holistic view supported by a systems approach exists. Working, funding, and managing information and knowledge differently will allow us to connect global health with global sustainability and national security as one. I especially acknowledge the patience, kindness, and professional contributions of Ms. Debby Nowicki, the IEEE issue editor, who offered her assistance to me in a big way and to the EMBS community by extension for helping me with the arduous and immense task of compiling this special issue. Once again, I thank John Enderle for his ongoing positive outlook, enthusiasm, and encouragement.

Luis Kun received his B.S.E.E., M.S.E.E., and Ph.D. degrees in biomedical engineering, all from UCLA. He has been the director of medical systems technology and strategic planning at Cedars-Sinai Medical Center in Los Angeles, the senior IT advisor to the Agency for Health Care Policy and Research, and the lead staff for High-Performance Computing and Communication (HPCC) Program and Telehealth. He is currently a senior research professor of homeland security at the Information Resources Management (IRM) College of the National Defense University (NDU), where he is the course manager for Homeland Security and Critical Infrastructure Protection. He has coauthored the Reports to the Congress on Telemedicine, in 1997, and on Health Insurance Portability and Accountability Act (HIPAA) Security. In July 1997, he was an invited speaker to the White House. He was largely responsible for the telemedicine portion of the bill that became part of the Balanced Budget Act of 1997, and he represented the DHHS Secretary at a Pan American Forum of Health Care Ministers on Telecommunications and the Health Care Industry in Mexico in 1997. In 1999–2001, as a distinguished fellow at the CDC, he has been the senior computer scientist for the Health Alert Network for Bioterrorism and later the acting chief IT officer for the National Immunization Program (NIP). He was an expert witness to Congress on HPCC and was the IEEE Health Care Engineering Policy Committee Founding Chair of the Electronic Medical Record (EMR) and HPCC Subcommittee. He is the founding chair of the Bioterrorism and Homeland Security Working Group for the MTPC and the Critical Infrastructure Committee for IEEE-USA. He is the chair of the Citizens Security and Safety for the International Federation for Medical and Biological Engineering (IFMBE). In the past 30 years, he has written and edited many articles and book chapters or sections. He is currently a coeditor of 2008 Careers in Biotechnology and Bioengineering (Springer) and the editor-in-chief of Handbook of Biomedical Information Technology (Elsevier). He has been in the IEEE Distinguished Visitor program for both the Computer Society and the EMBS and on the advisory board of many magazines and professional journals as well as associations and organizations [e.g., IEEE Transactions on Information Technology in Biomedicine, Informedica, Autism Talks, and International Council on Medical and Care Compunetics (ICMCC)]. He has lectured on medical and public health informatics, IT, and biomedical engineering in more than 60 countries. He has made numerous seminal contributions to the IT discipline. Among the many awards he received is the 2002 IEEE-USA Citation of Honor Award “for exemplary contributions in the inception and implementation of a health care information technology vision in the United States.” He serves on the Board of Directors (BOD) of the American Association of Engineering Societies and has served on the BOD of American Institute of Medical and Biological Engineering (AIMBE). In 2008, he was elected to the Board of Governors of the IEEE Society on Social Implications of Technology. He is a Fellow of the IEEE and the AIMBE.

Address for Correspondence: Luis Kun, Systems Management, IRM College, National Defense University, 300 5th Avenue, SE, Building 62, Fort McNair, Washington, DC 20319 USA. E-mail: KunL@ndu.edu.

References