



National Information Technology Priorities

A discussion of strategic IT priorities for the next several years in support of the U.S. Government's intent to bring focus and development to key technologies,

Enabling access to government human, physical and logical resources.

Abeezar Tyebji, CEO and Founder, Shipcom Wireless, Inc.

atyebji@shipcomwireless.com Cell: 713 302 3825

John C. Shoemaker, President, Shipcom Wireless, Inc

Contribution by Stephen Miles, MIT Auto-ID Labs

www.shipcomwireless.com

With the formation of President Elect Barack Obama's Federal Government Working Group that is focused on technology, innovation and policy reform, there is much discussion about what the priorities should be and how the new office of the CTO would bring results for the benefit of all. The media has reported that, "Obama's innovation agenda seeks to 'leverage technology to grow the economy and create jobs.' In addition, the agenda includes a wide range of proposals for a more "open and effective government" and a renewed commitment to science.

The working group will be organized into four sub-teams: innovation and government; innovation and national priorities; innovation and science; and innovation and civil society. This paper will discuss innovative technologies and some priorities that can span across each of the sub-teams, but we will also focus on one of the national priorities, healthcare, as an example of how technology can be leveraged to change the game and move to a new dimension.

The brief job description states that the role of the CTO is "to ensure that our government and all its agencies have the right infrastructure, policies and services for the 21st century. The CTO will ensure the safety of our networks and will lead an inter-agency effort, working with chief technology and chief information officers of each of the federal agencies to ensure that they use best-in-class technologies and share best practices."

Assumptions

Fundamentally, the role of the CTO should focus on championing and developing technologies that have strategic value to the United States. This should not include getting involved in or being a driving force in political battles (i.e. the Patriot Act) or Geopolitical issues (i.e. China's interference with the Internet) or off shoring conflicts (i.e. India or China or NAFTA). Of course,



the CTO should be considered a resource and an expert to advise Congress, but not a vehicle for resolving these and other issues like them.

How to Champion the Development and Implementation of Technologies

If we look at how the Internet was developed right here in the U.S., it was done under the leadership and guidance of DARPA. As has been the case with much military and space advancement, major breakthroughs came from such focused funding and research. In the case of TCP/IP, the world changed from one in which hardware gateways were required to connect devices from different manufacturers, to one in which physical connectivity could be established from one point to any other point on the internet.

The CTO should be able to establish a research fund that would give this office teeth, rather than have it be another bureaucratic position with no real mandate or capability to deliver results rather than reports. The CTO R&D funding could be extended to the private sector directly and through Universities for targeted technologies.

This effort can be the glue that brings private R&D efforts together with educational institutions that hits several birds with one stone. Education is important and these institutions will also be promoting such learning and literacy even as they help develop it. The intent would be to encourage both basic research and practical implementations. Web 2.0 is the next level in the life cycle of the Internet, but most computing systems, certainly within the government, are a long way from what would be described as innovative, open or effective. What will be the next new Internet-like breakthrough?

Priorities

Consider these comments or ideas as worthy of the CTO Office:

Security and Integrity of our IT Systems

Everyone now sees the pervasive importance of security. More than ever, we need increased levels of security across the entire spectrum of our society. It includes the world of hackers, identity thieves, felonious acts of fraud and theft, and even more disturbing, the world of terrorists, be they religious, commercial or government backed. Security is far reaching so let me drop down to some key areas:

- **Identification:** how to identify people, assets and things. This includes a full range from credential management, ePassports, biometrics and more. We need a policy with standards and technologies that bring confidence and reliability.
- **Data Communications:** inside federal/state/local governments of the U.S. and in the private sector, we need secure communications for normal operations and for disaster/emergency situations whether over landlines, cell phones or the Internet.



Encryption standards, policies and capabilities must improve to capitalize on the digital age and the control and management of massive quantities of data that is overwhelming our ability to comprehend it all.

- Access Control: who gets access and when? This includes people, animals and vehicles and affects access into a room, a building, a state, across national borders and more. Such identity and passage must not restrict freedom, freedom of movement and rights..This concern can further be broken into specifying the structure of data models, whereby different layers of information can be exposed, and the formulation of security roles tied to security rules for access to different layers of information.

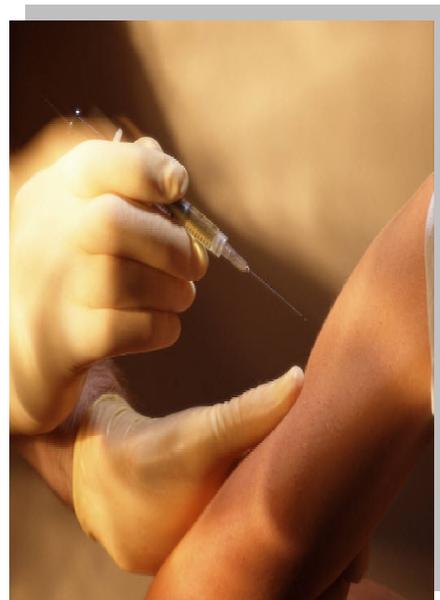
Wireless Technologies and Mobility

We are experiencing the mobile renaissance where mobile, handheld devices (PDA's, Blackberries, iPhones, generic cell phones and much more) are proliferating and gaining more power and capability each quarter. Device vendors such as Blackberry are working to ensure that their devices can meet the most stringent security standards. These wireless secure services should be made available to government employees, starting with the President.

- Integration with all aspects of IT internet based applications, ranging from banking services, messaging, to transaction processing and personal identification
- Support for the convergence of laptop computing and cell phones in both ubiquity and capability
- Standards that integrate or accommodate “best in class” service use of WiFi, WiMax, Cellular, Bluetooth, Zigbee, and more wireless transport networks.
- How to leverage RFID technologies like active and passive UHF, HF, LF, UWB and other microwave frequencies for identifying, locating and monitoring assets.

New Technologies

- With a DARPA like focus, develop partnerships that will spawn new technological breakthroughs. In effect, the CTO Office could be the national incubator for technological advancement.
- Provide vision and guidance for supporting technologies that will affect the top national issues facing the U.S. The CTO can impact other areas of the Government by leveraging





technology to reduce costs, streamline processes, deliver fast, secure communications, and even improve effectiveness overall.

- These issues have been described in several sources as:
 - Acquisition process improvement.
 - Budget management.
 - The war on terrorism.
 - **Healthcare.**
 - Energy and the environment.
 - Identity and access management.
 - Entitlement programs.
 - Disaster protection.
 - Financial and regulatory reform.
 - Government management.

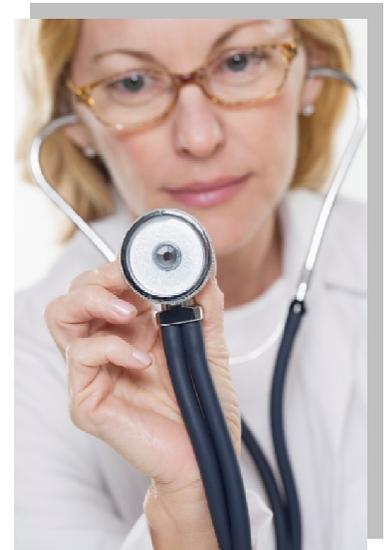
Economic Validation and Justification

There are many technologies that have been developed or are under development that are not being implemented because users have not been presented a ROI or financial justification. This is true no matter if the user is a government entity or a small private company. The office of the CTO should be able to muster the resources to qualify promising technologies and show proof of their financial value. In so doing, technologies could be evaluated and implemented more rapidly to the benefit of all concerned. Having a framework for financial or operational justification would be a huge step forward in gaining adoption well after the scientific and engineering work is done. Fundamental to effective government will be tools and information services that will assist government agencies in establishing and tracking their assets and liabilities such that they can be rolled up into one balance sheet for government operations.

We have learned that in the healthcare industry, adoption of technology that affects systems and processes has been slow. While there is much focus on specific products ranging from MRI's and CatScans to new drugs and implantable devices, there has not been a rush to incorporate technologies that change the way we provide healthcare. It seems that incentives must be established, clearly identifiable and measurable. Without it, technology gets bypassed for high profile inventions or cure-alls that get media attention and command high fees without addressing underlying healthcare ineffectiveness.

Focus: The Healthcare Industry

Our Healthcare Crisis





As noted above, Healthcare has reached a point that is now a strong national issue that has not been addressed to the satisfaction of few if any of the citizens of the United States. Past administrations and Congresses have dealt with it in various ways but now this area has gotten to the point where it is on President-elect Obama’s priority agenda.

“Making Patient Safety the Centerpiece of Medical Liability Reform” an article published in The New England Journal of Medicine by Hillary Clinton and Barack Obama, acknowledged the need for improved healthcare systems. “We all know the statistic from the landmark 1999 Institute of Medicine (IOM) report that as many as 98,000 deaths in the United States each year result from medical errors.¹ But the IOM also found that more than 90 percent of these deaths are the result of failed systems and procedures, not the negligence of physicians. Given this finding, we need to shift our response from placing blame on individual providers or health care organizations to developing systems for improving the quality of our patient-safety practices.

The opportunity is that this industry has not been aggressive to implement technology in ways that would reduce costs and streamline processes. One obvious example is that even after bar codes have been adopted for logistics tracking by industry around the world for years, bar codes are still not effectively used by many healthcare service providers. So the opportunity is excellent to bring a new dimension to healthcare effectiveness.

Critical issues include: availability, cost, delivery, and maintenance of healthcare services. When looking at technology for solutions that can address any of these points, one should see the clear benefits it can bring by addressing these areas of high importance:

1. **Patient Safety**
2. **Hospital/Healthcare Facility “Asset Visibility”**
3. **Medical Process Management and Industry Compliance (including HIPPA and JCAHO – the Joint Commission on Accreditation of Healthcare Organizations)**
4. **Staffing**
5. **Technology Standards (IT Standards for interoperability and integration)**

Addressing these issues will involve a hybrid approach to technology deployment. For example, bar codes, RFID active and RFID passive, Zigbee and UWB are all other forms of Automated Information Data Collection (AIDC) and monitoring technologies that could be managed from a single medical systems visibility platform. With the right technology capturing the relevant data

for processing by a process rules engine that interfaces to HIMS/DMLLS/HL7 type systems we can intelligently affect healthcare effectiveness. We can be proactive and innovative. We can reduce costs, increase patient safety while delivering a higher level of care and satisfaction.

1) Patient Safety

Healthcare providers understand the need to affect the 5 R’s: Right patient, right drug, right dose/amount, right time, and right delivery method. There are many aspects to bedside services which can be





addressed with technology that gives accurate and timely confirmation and recording of activity, but also confirms the 5 R's in real time to ensure the highest level of patient safety possible. With automation, we can reduce the role of human error and create an audit trail that provides visibility into what was done by who to whom and when...

To do this, existing technology combined with high level business process management specifications and integration to legacy IT systems can bring a new level of competence to healthcare processes and costs.

For example, by automatically identifying a patient whether in their bed or where ever they are in the hospital/facility, and automatically identifying and associating that patient with all other assets and caregivers of the facility will provide near real time visibility into healthcare services. It also can impact everything from patient safety to having an automated audit trail of procedures or services to verify what was done and by whom. Healthcare is beset with the problems of human error, but it does not stop there. Having the right machine, maintained properly, located in time and performing as needed is one aspect. Giving the right med to the wrong patient is obviously a problem, but also patient flow through ER is also critical. And there are so many other potential lapses or errors that have life or death consequences in a hospital. The statistics get worse each year.

The benefits of monitoring a patient's health is not restricted to identifying the patient and where ever they are located in the hospital, but also applies when they attempt to leave a facility. According to some estimates, by 2011 up to 50% of patients destined for assisted care facilities in the VA system could be accommodated in their homes through use of advanced personal medical devices that are being developed today. This level of patient security and connectedness is needed especially for babies, elders and those suffering for many types of illnesses or dementia.

2) Hospital/Healthcare Facility Asset Visibility

One of the applications getting more attention across all government functions is asset management; that is, tracking where assets are located throughout the facility/complex. Too much time is spent with caregivers running around trying to locate equipment needed for a patient. This covers the full range from wheelchairs to dialysis machines. Experienced personnel avoid this by hiding or hoarding equipment so they can readily access it when they need it. Unfortunately, this increases the need for more equipment and, in turn, increases costs overall. In order to mitigate against these losses the DoD has instituted the UID program. Extending





this mandate to cover healthcare assets would allow DHHS and their providers to track where their capital has been invested.¹

RFID (radio frequency identification) can be deployed to bring visibility in real time with an electronic dashboard that tells the location and status of equipment throughout the hospital to match equipment with medical needs quickly and with more effective use of resources. Almost the most simple of applications for this kind of technology, it also shows clear ROI and justification for management. This experience has been validated in the DoD RFID experience²

Asset management can extend to tracking and tracing any number of items in a hospital from the inventory in the pharmacy to the maintenance status of medical devices to ensuring the proper allocation of surgical instruments in specific kits. Any asset that moves or can move can be tracked and traced in real time with an asset visibility network in the healthcare facility. It goes well beyond theft prevention and asset allocation.

3) Medical Process Management



From the time the patient enters the hospital the paper trail becomes a burden throughout his/her journey from patient admission, to room assignment, medical services, testing and exams, procedures and then finally to discharge. Outpatient services demand more paperwork. The move to electronic or digital records will not only improve responsiveness and patient flow, but accuracy and timeliness of data.

Lots of work is being done on medical records, but they need fast, accurate and, at times, real time updates. There is a clear need to move away from paper files and records to digital maintenance of patient and other records, but currently medical service provider organization and physician efficiencies are not incentivized.

The computerization of data from electronic forms, electronic input to databases, and synchronization of data from devices will add to overall efforts to bring automation to healthcare while ensuring accuracy, integrity, and availability of secure personnel records where and when needed.

4) Staffing

¹ UID is a DoD program that enables improved access to inventory, repair, and deployment of items faster and more efficient:

² <http://www.acq.osd.mil/log/rfid/index.htm>





One recognized concern that brings pressure on healthcare costs are medical personnel. Therefore, anything that can be done to improve resource management while retaining key medical care givers will have enormous impact for all.

We are currently in a nursing shortage that is expected to intensify as baby boomers age and the need for health care grows. For the past decade, our military has been engaged in two wars and will like continue for many more years. This will ensure high levels of active and retired military personnel needing care for decades to

come.

According to the latest projections from the U.S. Bureau of Labor Statistics, more than one million new and replacement nurses will be needed by 2012. For the first time, the U.S. Department of Labor has identified Registered Nursing as the top occupation in terms of job growth through the year 2012.

www.bls.gov/news.release/ecopro.toc.htm

The National Council of State Boards of Nursing states the number of first-time, U.S. educated nursing school graduates who sat for the NCLEX-RN®, the national licensure examination for registered nurses, decreased by 10% from 1995-2004.

www.ncsbn.org

With the shortage of nurses and, as reported recently, interns working three shifts straight with little time for rest/sleep, the chances for error increases dramatically. Administrative burdens are continuously increasing. Many of these are due to JACHO regulations regarding frequency of patient to nurse interaction, frequency of nurse's hand washing, etc. Technology can provide automatic visibility to activities allowing more time for patient care.

Using technology from RFID to Mobile Messaging and specification of standardized interfaces can overhaul the administrative processes to streamline them and re-direct caregivers to more important and relevant tasks. Furthermore, as is being investigated in new initiatives within the Military Health System, mobile communications infrastructure can be repurposed for telemedicine applications that share expertise across organizational and even country boundaries.³

5) Industry Standards



³ Telemedicine and Advanced Technology Research Center (TATRC); http://www.tatrc.org/portfolios.html#health_information



Adoption of a new technology is always challenging. Some of the biggest issues are “interoperability” and standards. Industries are more likely to adopt a technology when it can be leveraged across multiple companies/facilities.

This has shown to be true many times in recent history such as cell phone handsets’ interoperability with different technologies such as CDMA, GSM, GPRS, etc. The military is especially adept at creating standards, but too often they are not interoperable across the various services.

Typical interoperability standards come about as a technology matures, adoption rates increase, and the most successful variation becomes prevalent or the “users” demand interoperability. It



is unnatural for commercial companies to work collaboratively to set standards, as each want to “own” the market or gain some competitive advantage or monopoly. Hence, proprietary solutions can be very efficient for a specific use or installation, but severely limits flexibility, alternative suppliers, entrepreneurial innovation and simple choice.

One approach that has proven successful is for several large companies and/or the Federal Government is to create mandates. There are several examples in the AIDC industry. In the mid 1980, bar codes were emerging but slowly. The AIAG and the DOD created mandates that standardized on Code 39 for all shipments and therefore allowed interoperability within their supply chain. Outside retail, Code 39 is the most widely used bar code in the world.

In early 2000’s, Wal-Mart and DoD created mandates for Passive RFID tags on all shipment based on specifications developed by the Auto-ID Center at MIT, working with the UCC bar code association. This created the EPC (electronic product code) Passive RFID Standard referred to today as EPC Gen II. This is the most prevalent UHF RFID tag in use today.

What will be the standard(s) for Healthcare? The Obama administration has the opportunity to mandate the standards that will drive adoption and increase patient safety/care while lowering healthcare costs. With any new technology adoption, continued work needs to be done to support standards at all levels of operations and administration.



Leveraging “nfc” Technology for Healthcare

Stephen Miles, a research associate for the MIT Auto-ID Labs (where the initiative to create the EPC Gen II passive “Far Field” RFID specifications originated) considers what would be required for leading healthcare life sciences companies, building on the success of the “contactless payment” industry, to leverage secure “Near Field” nfc “contactless” cell phone technology to acquire, authenticate and exchange patient medication and medical history data.

Research proposes to circumvent information barriers that have traditionally prevented patients from accessing and managing their personal health records through creation of a healthcare industry specification for use of “contactless” infrastructure for the authentication and secure exchange of personal healthcare data using “nfc” (near field communications) mobile phone apparatus.

The NFC cell phones reader/secure ID platform provides a ubiquitous interface to NFC Point of Sales (PoS) reader infrastructure that is being deployed by the payment processing industry worldwide for more secure payments. This same infrastructure can potentially be used to exchange medical records data with these same secure mobile phones. The nfc cell phone HF ID “tag” that customers use to make a “contactless payment” by a menu selection of credit card vendors including American Express, Discover, MasterCard and Visa at Point of Sale (PoS) “readers” at retail locations worldwide, could be used for patients to collect, store and share data with their medical service providers. The proposed cell phone platform also provides a secure interface to input medical device output into a HL7 Continuity of Care Document (CCD) personal health record framework⁴ such as are being instantiated in Microsoft HealthVault, Google Health, as well as healthcare payer and service provider patient record portals.

The barrier to medical services information exchange is nowhere more apparent than in the proprietary business processes that medical insurers, payers, processors and providers use to exchange an estimated 200 billion financial transactions per annum, of which 20% require manual intervention today according to John Hammergren’s “Skin in the Game...”⁵ By providing

⁴ HL7 Continuity of Care Document (CCD) ...

⁵ Skin in the Game: How Putting Yourself First Today Will Revolutionize Health Care Tomorrow; by John Hammergren (Author), Phil Harkins (Author);



patients with a user initiated mobile phone menu option to select health care portals and with whom to share healthcare information, the mobile phone becomes a platform to collect medication and medical history as well as medical device input. The objective of the MIT NFC Healthcare Applications Consortium is to provide a framework for shared information, algorithmic best-practice standardization and process improvement capabilities, through engaging users in taking control of their health services information via the cell phone.

A project has recently been defined and involves collaboration with Principle Investigators from the MIT Engineering Systems Division, the Harvard-MIT Division of Health Sciences and Technology and Beth Israel Clinical Research. Research issues include the interface of the mobile phone to large distributed IT systems in the complex medical care industry and for the use of the phone in a clinical setting as a platform for integration and management of medical device patient data.

Several issues have come to light in the investigation of cell phone interfaces for patient centric healthcare data exchange with front end Point of Sale readers and/or back end systems:

- Lack of industry identifiers for nfc cell phone based applications at the retail and/or service provider Point of Sale (i.e. how does a reader differentiate between a request for payment and a healthcare information exchange request)
- Lack of agreement for common cell phone interface by the healthcare portals
- Lack of security model that allows one patient or provider to initiate or terminate an account without impacting other providers using the same media
- Lack of agreement on a patient identifier, or the structure for such an identifier

One proposed approach leverages the Global Platform security specifications from the Smartcard industry as adopted in the US for ePassports and by DHS and the TSA for the Transportation Worker Identification Credential (TWIC) as advocated by the E-Authentication Federation (EAF) for U.S. government agencies. The recently ratified HL7 specifications for the Continuity of Care Document (CCD)⁶ for data exchange; and The Common Framework for Networked Personal Health Information: Overview and Principles are critical elements in enabling secure, efficient and cost effective healthcare data exchange.⁷ This approach has been covered in Stephen Miles Technology Disclosure with MIT Technology Licensing Office M.I.T. Case No. 13143 with the intent of creating an Open Source Framework to enable mobile phone based healthcare applications that support patients and providers in monitoring and making better healthcare decisions.

⁷ <http://www.connectingforhealth.org/phti/#guide>





Appendix

Contributing Factors Impacting the Nursing Shortage Enrollment in schools of nursing is not growing fast enough to meet the projected demand for nurses over the next ten years. Though AACN reported in December 2003 that enrollments in entry-level baccalaureate programs in nursing increased by 16.6% over the previous year, this increase is not sufficient to meet the projected demand for nurses. In a report published in the November/December 2003 issue of Health Affairs, Dr. Peter Buerhaus and his colleagues found that because the number of young RNs has decreased so dramatically over the past two decades, enrollments of young people in nursing programs would have to increase at least 40 percent annually to replace those expected to leave the workforce through retirement.

www.healthaffairs.org

Volume 354:2205-2208

May 25, 2006

Number 21

Making Patient Safety the Centerpiece of Medical Liability Reform

Hillary Rodham Clinton and Barack Obama

We have visited doctors and hospitals throughout the country and heard firsthand from those who face ever-escalating insurance costs. Indeed, in some specialties, high premiums are forcing physicians to give up performing certain high-risk procedures, leaving patients without access to a full range of medical services. But we have also talked with families who have experienced errors in their care, and it has become clear to us that if we are to find a fair and equitable solution to this complex problem, all parties — physicians, hospitals, insurers, and patients — must work together. Instead of focusing on the few areas of intense disagreement, such as the possibility of mandating caps on the financial damages awarded to patients, we believe that the discussion should center on a more fundamental issue: the need to improve patient safety.

We all know the statistic from the landmark 1999 Institute of Medicine (IOM) report that as many as 98,000 deaths in the United States each year result from medical errors.¹ But the IOM also found that more than 90 percent of these deaths are the result of failed systems and procedures, not the negligence of physicians. Given this finding, we need to shift our response from placing blame on individual providers or health care organizations to developing systems for improving the quality of our patient-safety practices.²

