Healthcare Information Technology and United States Healthcare*1

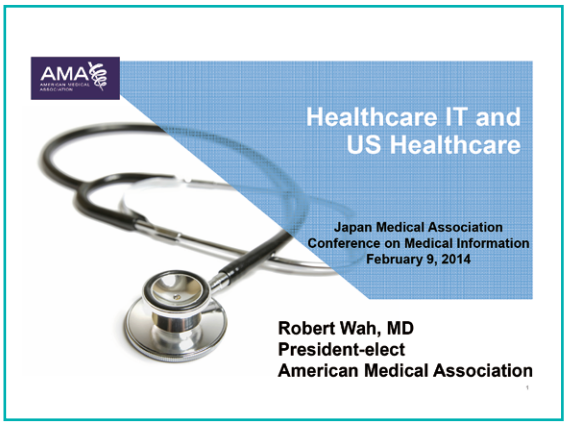
JMAJ 57(2): 84-92, 2014

Robert WAH[1]

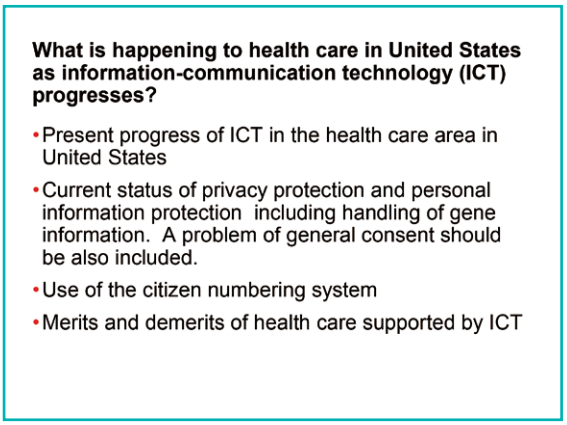
[Slide 2] As Dr. Shin of the Korean Medical Association mentioned, we were given several questions to answer in our presentations. I will also try to follow along the same questions that the JMA provided to us, the American Medical Association (AMA).

As way of background, I am a reproductive endocrinologist dealing with infertility and hormonal disorders in women. I live in the Washington DC, and I practice at the National Institute of Health in the Walter Reed National Military Medical Center in Bethesda, Maryland. I have spent my entire career taking care of women and their healthcare needs, and I have become very active in the area of Health IT in the last 10 years or so. I was the Associate Chief Information Officer through the US Department of Defense, where I worked as the lead doctor for the IT section, taking care of 10 million patients in 65 hospitals and 450 clinics worldwide. In 2005, I was loaned out of the Department of Defense to the Department of Health and Human Services, where I was the first Deputy National Coordinator for Health IT for the United States. In that role, I was the Chief Operating Officer, setting up a new office in the United States, called the Office of the National Coordinator for Health Information Technology. As the Chief Operating Officers, my job was to set up the new office, develop the strategy for the United States for the use of Health IT across the country. We had a new office with very little money—and we said "we have big dreams and no money." I'll tell you later what happened at our office.

In 2006, I left that office and retired from the military after 23 years on active duty service in the United States Navy. I am currently the Chief Medical Officer at the Computer Sciences Corporation. We do about $2 billion of work per year in Health IT around the world, and some



Slide 1

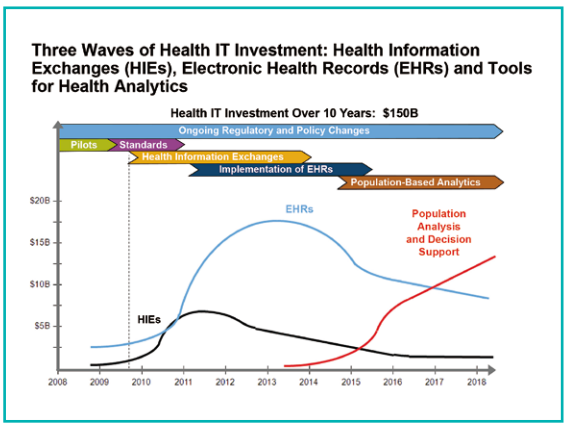


Slide 2

*1 This article is based on the lecture at the JMA Conference on Medical Information Technology held on February 8-9, 2014.

1 President-Elect, American Medical Association, Chicago, Illinois, USA.

Slide 3



Slide 4

of the largest deployments of electronic medical records were done by my group. We deployed electronic records to 2,500 outpatient clinics in the United Kingdom, taking care of 35 million citizens all on the same electronic health record system. So, this is the basis by which I present this information to you, not only about the United States but also about the global work in Health IT.

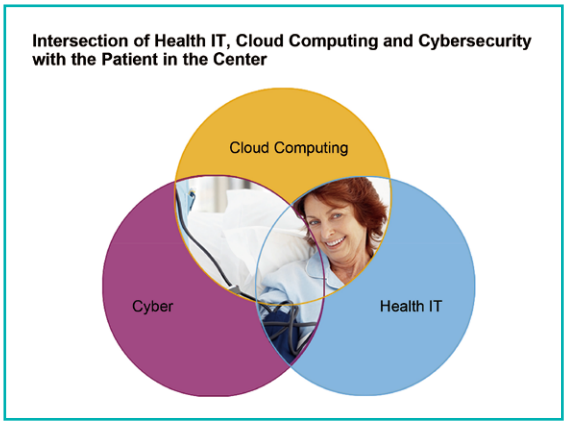
[Slide 3] It's my belief, from my experiences, that the role of Health IT is that it can actually transform healthcare by delivering better information for better decisions. Everybody in the healthcare space can use better information. Patients need better information. Doctors need better information. Government and insurance plans need better information. Researchers need better information to find new discoveries to help us take better care of our patients.

Technology, I believe, is a tool that helps us as doctors take better care of our patients. Dr. Shin talked about the concerns about interfering with the doctor-patient relationships. We as physicians must make sure that we use technology as another tool, just like we do in the operating room or in the clinic to take better care of our patients. We must not let the technology take over us. We must remain masters of the technology and use it as another tool to help us take better care of our patients.

Let me talk about what has happened in the United States in the last several years. As I said, I set up an office called the Office of the National Coordinator in Health Information Technology in 2005. I left the office in 2006. In 2009, the United States passed a new law called the Health Information Technology for Economic and Clinical Health Act (*a.k.a.*, the HITECH law), and that office that I started in 2005 was given $2 billion USD to do its work. I did not have $2 billion when I started the office in 2005—the budget was much, much smaller than that. In 2009, we also passed a law to provide incentive money for doctors and hospitals to move from paper records to electronic records.

[Slide 4] I made this slide around 2009, which describes what would happen over the next 10 years in the hi-tech path. I expected 3 waves of investment to happen in Health IT.

First, there is the investment in electric health records (EHRs), where we are going to invest somewhere in the neighborhood of $30 to $40 billion to get doctors and hospitals off of paper records and onto digital records. That is still happening today; doctors can qualify for between $40,000 and $60,000 per doctor to leave paper records and move to electronic records. Hospitals are given incentives in the order of $2 to $10 million to go from paper records to digital records. So, in total, something on the order of $30 to $40 billion will be spent on the migration from paper records to digital records. Now, the Office of National Coordinator also has $800 million to a billion to network these digital records together into what we call the Health Information Exchanges, or HIEs, which is the second wave of the investment. So now, we are going to get off of paper onto digital records, and we are going to network those records together



Slide 5

Slide 6

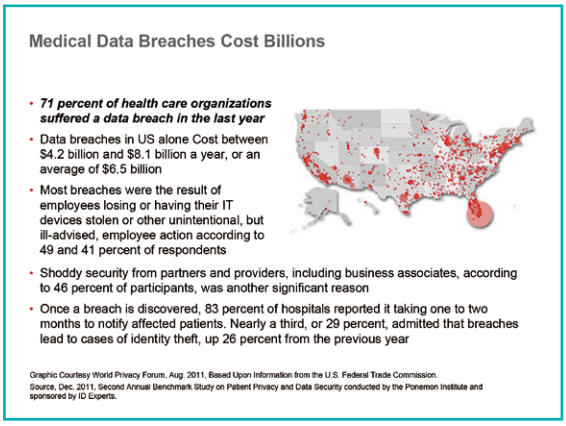
and form these HIEs. It was my belief in 2009, that we are going to see the third wave of investment happen right around now. Now that we have digital information that are networked together, we would want to analyze that information and support decision-making to help physicians take better care of their patients. The first 2 waves have already happened, and now, we are starting to see the rise of the third wave.

[Slide 5] It is also my belief that we are seeing an intersection and overlay of 3 major technologies. One is Health IT, and the second is a new technology called Cloud Computing. The third technology, and a very important component of this intersection, is what I call cyber security or technology, to prevent the release or hacking of information. Our patients is in the middle of this intersection, and we should never forget that that is why we are doing all these things—we are not doing our work for technology sake, we are doing it so we can take better care of our patients.

[Slide 6] Let me break each one of those intersections down, and just talk briefly about what each means to me as a practicing physician using technology to take better care of my patients. Cloud Computing has a lot of different meaning to a lot of different people. In many ways, it involves being able to episodically use just the right amount of computing power that you need—not too much, and not too little. It also means that information is now much more fluid and moves around in new ways that we never were able to do before. In the old classic, there was a big box inside of a big building, called a computing center. Now, with Cloud Computing, the computing can happen very far away from where the user needs to have the information. By separating where the computing happens and where the user utilizes the information, it gives us many new opportunities to change the way we use information and take care of our patients.

One example of that is, all of our devices—a computer in your desk or a handheld in your pocket—now can serve as a window or a viewer into the computing activity, which can be happening hundreds or thousands of miles away from where you are using the information. So, as I said before, there is a continuum now. It could be a desktop computer or a borrowed computer of your aunt's house. You could be in the office or a hotel or at an airport. You can be on your handheld or tablet. It does not matter where you are; you have access to new information because these devices are just a viewer into the computing that is happening somewhere else.

Let me change gears now, and talk about cyber security. Dr. Ishii and Dr. Snædal both mentioned our concern of our patient's privacy, of the important information that they have given us. We, as physicians, have always been what I call *data stewards*. Our patients come to us, and they tell us some of the most confidential and private information about their lives. They do that very willingly because they trust us as physicians, to hold that information private and confidential. They know that telling us that private and confidential information will help us take better care of them. So, for centuries, physicians have been entrusted with private and confidential information. We, as physicians, must



Slide 7

continue to protect our patient's private and confidential information, even though that information has now left paper and is now on a digital platform. I will tell you, however, that now that we have moved to a digital platform, there are new threats to the privacy and confidentiality of patient information.

When we used paper to keep patient information, we had to try to keep it private inside our offices or inside our hospitals. That was thought to be fairly private. If you think about it, however, in some ways paper records are not protected very well because there is no record of who looks at a piece of paper. Anybody—the doctor, the nurse, the front desk clerk, or even the janitor who works in the building—can look at a paper record, and there is no trace of that. So, in some ways electronic records give us a new layer of protection, because we can protect the digital information by making sure there are digital footprints by anybody who looks at a digital record.

Now, some of the things that we talk about in terms of privacy and security are along the lines of protecting the patient's private information. For example, I am an obstetrician gynecologist, so many women are very concerned that their reproductive history may get out. If they have had pregnancy termination or sexually transmitted diseases, it can be potentially very embarrassing and damaging if this information gets out. In other specialties, for example if a patient is on a psychiatric medication or has had counseling for psychiatric diseases, it is often very concerning for patients if that information were released.

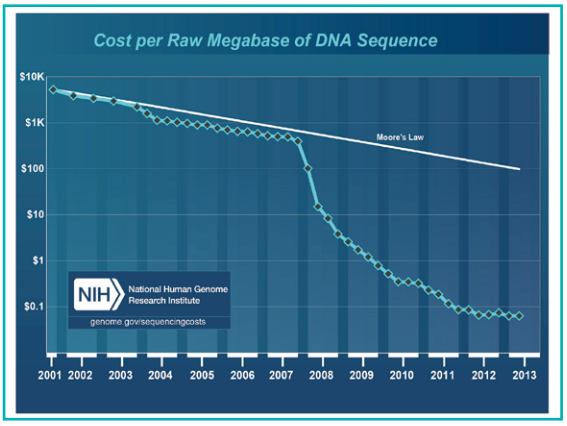
So, patients are very concerned about breaches. If you ask them about digitalization of healthcare or Health IT, their number one concern is that their health information will show up on the internet. We have all seen that credit card information can show up on internet, but health information can be very much more damaging if it is exposed. If your credit card shows up on the internet, it is a big problem, but a solvable one. It might take a couple of years, tons of phone calls, and many hours of work, but you can overcome the damage of your credit card information showing up on the net. However, if your critical health information, *i.e.*, your diagnosis of HIV infection, the fact that you are on psychiatric medication, or the fact that you have a sexually transmitted disease, shows up on the internet, that is a bell you cannot un-ring. Patients know that, and they are very afraid. So, they expect us in the health field to take very, very careful care of their private and confidential information. So, that is one part of privacy and confidentiality about the Health IT movement that we are seeing.

Now, I will tell you that there is a whole another side to that. **[Slide 7]** This is a list of some of the medical data breaches that have occurred in the United States in 2011. It is very widespread and expensive. Just very recently in the United States, we have heard a lot about organized crime trying to break in and get credit card information. In the holiday season in the last winter, a major store in the United States called Target had somewhere between 40 and 100 million records stolen by criminal elements who wanted to gain access to the financial information in those credit cards and debit cards. I believe it made the newspapers everywhere around the world. In healthcare, those same criminal elements are trying to get your health information as well. They do not care about your diagnosis of HIV or your sexually transmitted history; their interest is in the street value.

[Slide 8] On the street, the criminals can sell credit cards for about a dollar per credit card number, but they are currently selling health records for $15 to $20 per record. Health records are much more valuable than a credit card number, because a health record is so rich in information about a patient that you can create a very strong identity with that health information,

Slide 8

Slide 9



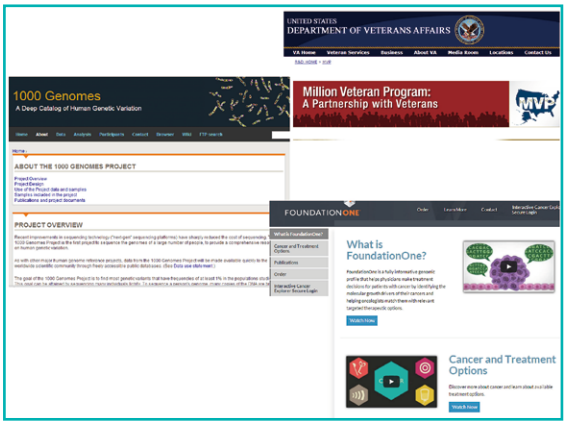
Slide 10

and with that strong identity you can earn much more in financial fraud than you can with a single credit card number.

So, we are now under attack in healthcare by the same criminal elements that are attacking financial information, and we in healthcare need to start utilizing the same industrial-strength technologies that are used in the financial system. Granted, those technologies are not very good, because we still see breaches like we saw at Target where 40 to 100 million records were accessed. Nevertheless, across healthcare we are not anywhere close to the cyber security levels that banking and financial institutions use, and we in healthcare need to start thinking about the fact that we are under attack by the same criminal elements that those financial institutions are being attacked by. My point is, we need to be mindful of our role as *data stewards* in protecting the privacy and security of our patient's information, not only for their health reasons but also to fight against these criminal elements that are seeking to attack the massive information that we have built up in healthcare.

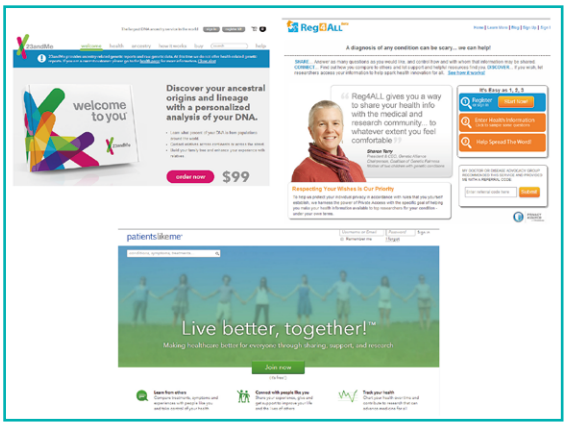
[Slide 9] My last comment about security and privacy is that many people see privacy and security as a burden, as one more thing they have to do, and that it is a cost. Let me try to make a different argument for you. At the company I work at CSC, we protect the secrets for all the 3-letter organizations in the US governments, such as the CIA, the NSA, and the FBI. The cyber security experts of my company tell me that we need to think of security not as a burden but as an enabler, because without security we will not be able to have a network. If patients are concerned that we do not have adequate security, they will stop giving us information. Then, the networked electronic digital platform we talked about will cease to exist, and all those benefits that we hope to reap from having access to that information will go away. We need to think of security as an enabler that makes patients, doctors, and governments comfortable in having a networked digital information system. So, we need to stop thinking about security or privacy as a burden or cost. We need to consider it as an enabler that gets us where we want to be, which is having networked digital information available to help us take better care of our patients.

I want to switch gears now because we were asked to talk about genetic information. **[Slide 10]** This is a slide presented by the National



Slide 11

Slide 12



Slide 13

Institute of Health, one of our premier research institutes in the United States, which describes the rapid decline in the costs of performing genetic analysis. We use this line that represents the Moore's Law as the reference. He was one of the co-founders of the Intel Corporation that makes the chips in many computers. A long time ago, he made a statement that every 2 years the computing capacity on chips would essentially double. For years and years, this Moore's Law has almost been like the law of gravity—every 2 years, our computing power has doubled. If you think about it, that is a tremendous achievement. We have never doubled anything every 2 years except for computing power.

Let's look at what we have been able to do in genetic analysis. The cost of performing a DNA sequencing has dropped precipitously in just last 7 or so years, to the point now that there is a new proliferation of companies and activities based on the fact that we can get very rich information from genetic analysis. **[Slide 11]** I will show a series of slides very quickly to give you some examples. I do not have the time to go into a lot of detail, but I wanted to show you some of the activities that are happening around the United States. The Veterans Administration,*2 which is for all the people who have left the military, are seeking to get the DNA from 1 million veterans to start a DNA database of a million veterans. There is an international project called 1000 Genome Project,*3 which is starting a library of genetic analyses from 1,000 people with diseases to compare against when we find out the genetic makeup of other individuals. The FoundationOne*4 is another group that specifically started looking at cancers to find out if we can tell the genetic makeup of a cancer cell in order to figure out what is the best treatment for that cell—not all the other ones, just that one particular cell. **[Slide 12]** The Partners Healthcare*5 is a hospital system at the Harvard Medical School, and they are now offering services that are based on the entire genome analysis of a patient. The Illumina*6 is another group that is seeking to help doctors take better care of their patients with a definitive genetic analysis of the entire genome.

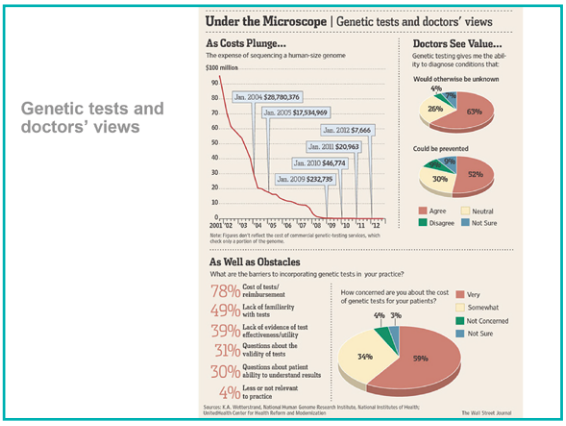
[Slide 13] Now, I want to switch to another slide, which talks about what patients think

*2 http://www.va.gov/; *3 http://www.1000genomes.org/; *4 http://foundationone.com/; *5 http://www.partners.org/; *6 http://www.illumina.com/.

about their own private information. As I said before, patients are very concerned about their information showing up on the internet. However, there are some interesting activities on the patients' side, which tell me that there is a change in the way we need to think about patient's information as well. The first example I would like to share is a company called 23andMe.*7 They send you a small kit in the mail, and you take a swab of your inside cheek and send it in, and for $99 they will give you a genetic analysis not of your entire genome but just certain parts of it. They were just asked to stop being a healthcare advisor, and they are now only allowed to tell you about your relatives that have the same kind of genetic changes that you have. So, patients now have the ability to obtain genetic information about themselves and their families for $99.

This group here, Registrations for All, or Reg4All®,*8 is a company where patients are willingly giving information. It is not necessarily genetic information; it can be a history of their diseases, their surgeries, or their medications. Patients share those information to see if there are other patients like them who can share information, and figure out how their disease, either chronic or serious, can be bettered by sharing information with others.

The last one I would like to mention is a company called PatientsLikeMe,*9 which was started by an engineer of the Massachusetts Institute of Technology (MIT) whose brother had been diagnosed with a fatal disease called amyotrophic lateral sclerosis. As those of you in neurology know, this is a fatal, debilitating disease, where you lose the function of your muscles very gradually at first but then very rapidly, so you can no longer move or speak, and ultimately you can no longer breathe. The brother started a website because he was very frustrated that there were no good therapies for his brother's fatal disease. So, he started up a website called PatientsLikeMe, and other patients with this unusual and fatal disease started posting very personal information. They would post their X-rays, blood test results, and doctor visit summaries—to help see the other patients out there who had the same disease, that maybe others had a different outcome or a new success.

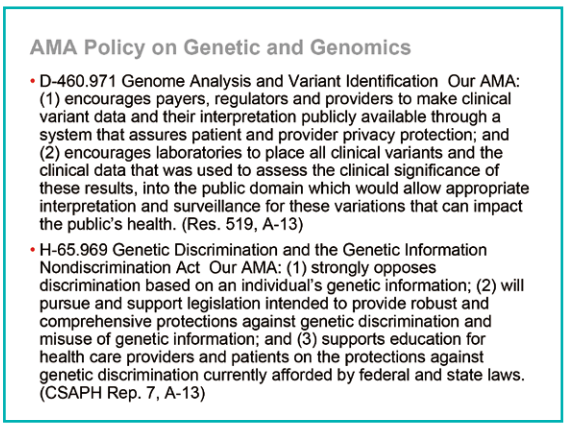


Slide 14

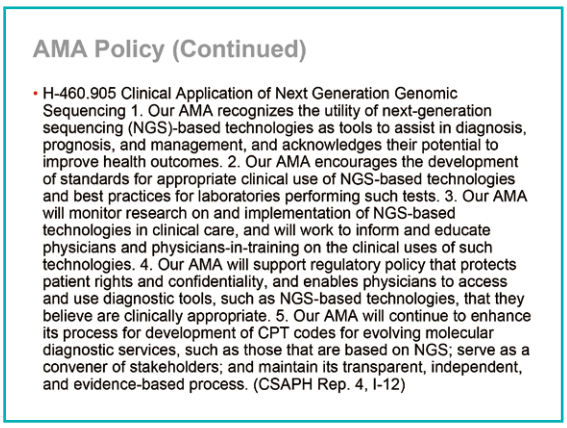
This MIT engineer adamantly believes that privacy laws are killing patients every day. He says that the fact that we keep all this information private rather than sharing is killing other patients around the world. In his belief, interestingly, the last thing you worry about when you are sick is the privacy of your information. So, when you have a fatal cancer or disease that you know it is going to kill you, the last thing you care about is whether or not other people know your private information. In fact, at that point, he encourages to share all your information, and see if others in the world have had a same disease but had more success than you have with other medications or other therapies. So, this website is a very open website where people share their most personal information, down to the degree of what they ate for breakfast or what their temperature was at noon. They are putting all up on the website, in the hope that somebody else could benefit from it or somebody would give them advice to help them. So, it is a total change in the way we see privacy and security. I believe that the difference is in the status of your own health; when you are healthy, you have a different perspective on privacy and security than when you are sick, especially with a fatal disease.

[Slide 14] This is a quick chart about what doctors in the United States think about genetic testing when asked by the Wall Street Journal. The first thing you see is how rapidly the cost of genetic analysis has plunged, even faster than

*7 https://www.23andme.com/; *8 https://www.reg4all.org/; *9 http://www.patientslikeme.com/.



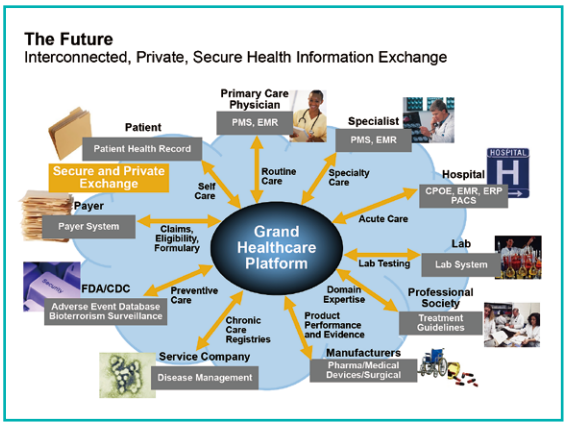
Slide 15



Slide 16

the Moore's Law would have predicted. This chart stopped in 2012 at $7,000, but we believe the cost of a genome analysis would be a $1,000 or less in the next 12 to 18 months. That shows how rapidly the cost is coming down. So, genetic analysis will give us a whole new suite of information we never had before, which we can use to take care of our patients. These other charts are about what doctors think about in terms of genetic testing in particular.

[Slide 15] Now, I want to switch the topic and talk about the policies that we made at the AMA, specifically in the area of genetic testing and the use of information. I believe it falls into a couple of main areas. One is, we obviously want to be very careful that clinical information about genomes does not become too private and too proprietary, where a company is going to start making money because they have genetic information that they only share if you pay for it. We want to make sure that the genetic information is a much more open and shared, so that all of society can benefit from new discoveries in the area of genetic testing and genetic information. We also want to make sure that our patients are not discriminated against. Many times genetic information does not tell you exactly what is going to happen to you, but it might tell you that you are at increased risk of suffering a certain disease. So, there is a concern that patients will be discriminated against for having certain genes. If you have a gene that says you are at an increased risk for a disease, employers may fire you, or the insurance company may stop insuring you or may charge you more for your insurance.



Slide 17

We consider that discrimination simply based on your genetic makeup is possible, and it concerns us very much.

[Slide 16] Another AMA policy I have here, again, talks about making sure that we as physicians embrace this new technology in a way that will help us take better care of our patients. That means training our new doctors in medical school, our existing doctors in practice today, and the rest of the medical industry about how we can really take advantage of this new source of information about our patients. So, this is a quick summary of some of the major policies that we made in the area of genetics at the AMA.

[Slide 17] In summary, let me just talk about what I see in the future of IT in healthcare. I believe that we are all going to start forming what I call the Grand Healthcare Platform, which is in the main circle at the middle of the

Slide 18

slide. It is not a physical place or a physical thing; it is a virtual pool of information. All of us in healthcare—patients, doctors, nurses, specialists, hospitals, labs, societies, manufacturers, government—are around the main circle. Everybody will want to contribute to the pool and take out different information from the pool, but we will be in and out of the pool all the time. The arrows pointing to and from the pool are the pipes that get us to and from this pool of information, and this is where I believe we can build industrial-strength cyber security to make sure that appropriate use of this pool is enforced. We have all the ethical and legal considerations that were mentioned by the 2 previous speakers. We need to make sure that the access to this pool is very controlled and secure, in both getting the information in and out. However, this pool of information is not going to be one big database or one big computer in the sky. It is going to be information in multiple places, but we can assemble it together as if it is one virtual pool using technology.

Soon, we will be going in and out of the pool to help us take better care of our patients. It may be to coordinate the care of our patients across specialists, learn new discoveries about how to take care of chronic or lethal diseases, or allow our patients to participate in their own care in ways they never were able to do before. So, this virtual pool of information is forming today, and we never would have been able to have that so long as we had health information solely on paper. We are living in an age that the paper-based system is giving away to a new digital system, and that digital system is now networked together forming this virtual pool of information. It is incumbent on us to use the cyber security technology to protect the virtual pool of information, or else the patients will not let us have it anymore. That is where I believe we are heading very quickly.