CYBERSECURITY, ANALYTICS & MORE:

The 8 Government Health IT Trends You Need to Know

CONTENTS

Information Builders | Health

Business Intelligence

Better **Data.**
Better **Analytics.**

Clinical, operational, financial analytics for healthcare backed by a single trusted view of data across your entire health network.

Data Integrity

Data Integration

EXECUTIVE SUMMARY

Health information technology makes it possible for health care providers to better manage patient care through secure use and sharing of health information. Health IT includes the use of electronic health records (EHRs) instead of paper medical records to maintain people's health information.

More and more, health care providers are using health IT to improve patient care. But health IT isn't just for health care providers. Patients can use it to better communicate with their doctors, learn and share information about their health, and take actions that will improve their quality of life. And as the scope of health IT grows, government — the world's largest IT customer — is driving the adoption of IT in health care.

You may be wondering: What exactly does the government have to do with any health technology that may affect me? Well, clearly the government does not dictate what system doctors or hospitals should use or what types of health IT to invest in. But as HealthIT.gov states: "The government is involved because health IT supports cost-effective ways to improve the quality of care. The government's role in health IT includes:

- encouraging adoption,
- supporting information privacy,
- supporting research on the appropriate use of health IT, and
- using health IT systems in government-operated hospitals."

This GovLoop guide will look at the current state of government health IT, innovations and how government is driving the adoption of IT in health care.

Read on for a look at the Federal Health IT Strategic Plan, eight trends in government health IT today, and spotlight interviews with movers and shakers in public-sector health technology.

A LOOK AT THE FEDERAL HEALTH IT STRATEGIC PLAN

The biggest driver of the federal government's health IT approach is the Office of the National Coordinator for Health Information Technology (ONC). ONC is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health IT and the electronic exchange of health information.

In late 2015, ONC released its strategic plan for 2015-2020, representing an "action plan for federal partners, as they work to expedite high-quality, accurate, secure and relevant electronic health information for stakeholders across the nation," wrote National Coordinator for Health IT Karen DeSalvo on the ONC website.

This strategic plan gives us insight into the current state of government health IT, and the path it's headed down.

For a better understanding of the strategy, we lay out its four main goals:

1. Advance person-centered health and self-management.
2. Transform health care delivery and community health.
3. Foster research, scientific knowledge and innovation.
4. Enhance the U.S. health IT infrastructure.

GOAL 1: ADVANCE PERSON-CENTERED & SELF-MANAGED HEALTH

↗ OBJECTIVE A:
Empower individual, family, and caregiver health management and engagement

↗ OBJECTIVE B:
Foster individual, provider, and community partnerships

GOAL 2: TRANSFORM HEALTH CARE DELIVERY & COMMUNITY HEALTH

↗ OBJECTIVE A:
Improve health care quality access and experience through safe, timely, effective, efficient, and person-centered care

↗ OBJECTIVE B:
Support the delivery of high-value health care

↗ OBJECTIVE C:
Protect and promote public health and healthy, resilient communities

GOAL 3: FOSTER RESEARCH, SCIENTIFIC KNOWLEDGE & INNOVATION

↗ OBJECTIVE A:
Increase access to & usability of high-quality electronic health information and services

↗ OBJECTIVE B:
Accelerate the development and commercialization of innovative technologies and solutions

↗ OBJECTIVE C:
Invest in, disseminate, and translate research on how health IT can improve health and care delivery

GOAL 4: ENHANCE NATION'S HEALTH IT INFRASTRUCTURE

↗ OBJECTIVE A:
Finalize and implement the Nationwide Interoperability Roadmap

↗ OBJECTIVE B:
Protect the privacy and security of electronic health information

↗ OBJECTIVE C:
Identify, prioritize, and advance technical standards to support secure and interoperable health information and health IT

↗ OBJECTIVE D:
Increase user and market confidence in the safety and safe use of health IT products, systems, and care delivery

↗ OBJECTIVE E:
Advance a national communications infrastructure that supports health, safety and care delivery

TREND #1

BETTER CYBERSECURITY AROUND HEALTH DATA

Cybersecurity is not a new issue, and today, it's more critical than ever, especially in government health IT. It refers to the very state of being protected against the criminal or unauthorized use of electronic data. In this case, cybersecurity in health IT is of particular concern because so much of the data that could be hacked is sensitive in nature.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

Ten years ago, the health industry might not have given much thought to cybersecurity. Most patient data and documents were not electronic and concerns about hacking weren't a priority.

How quickly things change. Today, because of electronic medical records (EMRs), the Internet of Things and the variety of connected health devices, the health care and health IT infrastructure that create efficiency have also created a vulnerable attack surface for hackers to come after.

An example? HealthCare.gov has logged more than 300 cybersecurity incidents in the past 18 months. And according to a report in USA Today, the health care industry has accounted for more than 40 percent of data breaches in the past three years, and 91 percent of all health organizations have reported a breach in the past two years.

Health data is more vulnerable than ever — and the government is starting to do something about it. In March 2016, the Health and Human Services Department announced a cybersecurity task force to study ways of protecting health data and connected medical devices following years of escalating cyberattacks on health information systems.

RANSOMWARE is responsible for

406,887

ATTEMPTED INFECTIONS & ACCOUNTS

for a total of

$ 325 MILLION

IN DAMAGES

[source]

HEALTH CYBERSECURITY IN GOVERNMENT TODAY

One cybersecurity issue that's exploding in the real world for health IT and health care providers? Ransomware. This is a type of malicious software designed to block access to a computer system until a sum of money is paid. And hackers are using it to target health systems and hospitals.

For example, earlier this year, a hospital in Los Angeles said it paid the Bitcoin equivalent of $17,000 to hackers after patient and doctor records were locked for almost two weeks. In the meantime, the hospital had to resort to handwritten records to cope with the computer lockdown.

That hospital's vulnerability was not an exception, either. A recent task force and report concluded that "hospitals are riddled with cybersecurity flaws that could allow attackers to hack into medical devices and kill patients."

The report explains that "hospitals have focused most of their cybersecurity efforts on protecting private patient records, and not enough on defending computer systems that are hooked up to patients and could be used to cause them harm."

WHAT'S NEXT?

The health industry has not always made cybersecurity a priority, but 2015 and 2016 will go down as the years that officials woke up to the very real consequences that cyberattacks could have on their infrastructure and patients' information.

Despite a growing response to better cybersecurity in health IT, attacks will continue at a possibly accelerated pace.

In addition to dealing with ransomware attacks, the rapid increase in connected devices in health IT will be of major concern to government health IT cybersecurity going forward, because it offers many more opportunities for hackers. Indeed, according to this article in *Becker's Health IT & CIO Review*, "experts suggest medical information is up to 10 times more valuable than financial information like a credit card number on the black market. Hackers can essentially sell identities using personal data on the black market, create fake identifications to buy medical equipment or drugs and file fraudulent claims with payers. Additionally, medical identity theft isn't always immediately apparent, so hackers have more time to use stolen credentials for fraudulent purposes, unlike credit cards which can be instantly cancelled upon fraud detection."

WHAT YOU NEED TO KNOW

#1: Connected devices in health IT are a new frontier for hackers.

As more devices connect to the internet — creating what is known as the Internet of Things (IoT) — the potential for hackers to access and hack them has grown.

#2: EHR security is still an issue.

Most EHRs and related equipment have security features built in or provided as part of a service, but they are not always configured or enabled properly.

#3: The government is working on it.

HHS has put together a collection of tips and information to help health IT users and professionals protect and secure health information that they may access, receive and store on mobile devices such as smartphones, laptops and tablets.

TREND #2

THE INTERNET OF THINGS

The Pew Research Center defines IoT as a catchall phrase for the array of devices, appliances, vehicles, wearable material and sensor-laden parts of the environment that connect to the internet and to one another and feed data back and forth automatically. In terms of health, it is the interplay among monitors, fitness trackers, implanted medical devices or any other object that transmits or receives data.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

Think of the human body as a car. For years, drivers have been able to monitor the health of their vehicles with oil and pressure gauges that give alerts when there is a problem. But unlike a souped-up BMW, patients with chronic medical issues lacked alerts for when a tune-up is needed. There was no caution light for diabetes or heart disease — until recently.

Doctors at the Veterans Affairs Department have been looking to use smart health care devices to make health care not only more accessible, but also more effective for patients. IoT-based health care innovations include fetal, heart, temperature and blood glucose-level monitors in addition to robotic mental health assistants. And it's not just VA investing in IoT solutions.

The Centers for Disease Control and Prevention, HHS, and many state health organizations are looking to IoT to provide better health care to patients in their homes. In addition to improving patient care, the use of IoT could save $63 billion in health care costs over 15 years with a 15 percent to 30 percent reduction in hospital equipment costs and a 15 percent to 20 percent increase in patient communications, an Atlantic Council report found.

Connected medical devices pose some serious challenges to the security and privacy of patients' health information, however. The devices beg the questions: Who owns the data? Who is authorized to act based on the data? And is the data secure? In large part, the medical field is still grappling with the answers.

***Forecasters say that by 2020**, about **4 BILLION** **MEDICAL TRACKING DEVICES** will be connected to patients for purposes of monitoring blood pressure, cholesterol, blood sugar and more.*

[source]

IOT IN GOVERNMENT TODAY

VA has been on the leading edge of connected devices for years. Right now the department is working on more than 50 internet-connected devices — everything from sensors that gauge a person's gait to monitor for future falls to robotic mental health providers.

One of the department's most promising projects is a prototype for a flu shot alert system that would prompt people entering their local drug stores to get a flu shot. "As the individual walks into the store, there is the capability through multiple platforms and geo-location to have an iPhone or an Android device prompt you that you are actually at a VA-approved location that can give you a flu shot," said Joseph Ronzio, Deputy Chief Health Technology Officer at VA.

VA isn't stopping at flu shot notifications. It's also looking at similar technology to monitor chronic illnesses. "Let's say you have your medical records on your device, and you have diabetes. There's blood work and tests you should have accomplished," Ronzio said. "Many convenience stores are getting into that market where they have mini clinics. Well, if we have contracts with them, patients can get an alert based on their medical information and their disease management protocols to go get the lab work done while they're there. So instead of having to make a trip to a lab, patients can handle their blood work right in the convenience store."

WHAT'S NEXT?

Despite the very real concerns of privacy and security, health IoT advocates point to the possibilities that such devices will to give patients. "[Data] has to be part of how consumers and patients think about their care experience," said Patrick Conway, Chief Medical Officer at CMS, at the annual Health Datapalooza in 2015.

By giving patients robust data, they are better able to make informed decisions about their health. For example, the University of New Hampshire is using smart beds that can detect when they are occupied and when a patient is attempting to get up. The smart bed can also adjust itself to ensure that patients receive the appropriate pressure and support without nurses' manual interaction.

Government agencies are also teaming up to help administer the field. The Food and Drug Administration offers guidelines for medical devices, and regulators will likely continue to control connected devices that patients use. HHS has also created an IT strategic plan to help agencies share information and collaborate on IoT.

WHAT YOU NEED TO KNOW

#1: Privacy will be paramount.

Privacy and cybersecurity around IoT will become even bigger issues than they already are, in large part because as its use grows rapidly, some significant security failures by large IoT providers are likely, bringing any privacy or security weaknesses to the forefront.

#2: IoT will need to be standardized in government.

A fully functioning IoT won't be of much use if standardization and a common framework for the billions of devices aren't put in place. Fortunately, the National Institute of Standards and Technology is working on such benchmarks.

#3: The interface matters.

IoT and its accumulated data will never truly take off in patient care or government until they are easy to use and understand. Apps and dashboards monitoring this data have yet to catch up with the data-gathering abilities, and that will be the next step for the government.

We make making the rounds easier.

Citrix Public Sector helps government IT healthcare agencies deliver patient information anywhere clinicians need it.

Government healthcare workers need patient information, and they need it fast. Citrix solutions provide some of the largest government healthcare agencies secure, instant access to electronic health records and patient data on any device, anywhere. That's better care when seconds count — at a serviceman's bedside, on the battlefield, or on call home or abroad.

See why more than 3 million healthcare workers rely on Citrix every day.

For information on Citrix healthcare solutions visit **www.citrix.com/health**.

CITRIX® Public Sector

©2015 Citrix Systems, Inc. All rights reserved. 4988 Great America Parkway, Santa Clara, CA 95054 USA.
All trademarks are the properties of their respective owners.

INDUSTRY SPOTLIGHT

ENHANCING MOBILITY & SECURITY FOR HEALTHCARE IT

An interview with Jose Padin, Sales Engineering Director, U.S. Federal Civilian & Federal System Integrators, Citrix

Creating a vision of health care technology that can support the health of all Americans in smart and efficient ways is no easy task. Though much progress has been made across the health IT market, several challenges still remain – everything from dealing with cybersecurity and interoperability issues to health care modernization and more.

To help government better understand these challenges and how to overcome them, GovLoop talked to Jose Padin, Sales Engineering Director, U.S. Federal Civilian & Federal Systems Integrators at Citrix Systems, a software company that provides server, application and desktop virtualization, networking, software-as-a-service, and cloud computing technologies.

Citrix is a key health care IT solutions provider with large scale customer implementations in government agencies, including the Defense Health Agency and the Department of Veterans Affairs. Citrix also has an extensive history of offering solutions focused on instant access to secure patient data, which helps solve the challenge of bringing together clinical and non-clinical applications for better collaboration.

"One of the biggest challenges today in government health care is modernization of electronic health record systems," Jose said. "There's been a lot of well-documented issues around patient care and providing the fastest service possible to our war fighters and veterans. Modernizing health records and improving secure access to them where and when they are needed is a critical challenge that we're seeing across both military and civilian health care."

A second challenge, Padin explained, is the ability to support and secure multiple IT devices – especially mobile ones – within health care facilities. "We've seen an increase in tablets and mobile devices inside health care facilities. Securing all these devices and making sure that patient data is accessible by only those who need it is a top priority to comply with HIPPA data privacy mandates."

Finally, a shortage of health care workers is a serious challenge to government health care service providers. Today, health care workers are mobile and need to be more efficient and effective with technology than ever before, so they can access patient data anytime and from any device seamlessly and securely.

"Efficiency is a critical priority," Padin said. "Anything that we can do to allow a health care worker to securely work wherever, whenever, and on any device, is now a critical priority in government health care. It's all about providing patients a good health care experience by enabling the mobile health care worker secure access to patient data. We need to balance patient care with a great technology experience and ensure patient data is as secure as possible."

So how can government overcome the many challenges they face in health care IT today? One way is by centralizing access across all government devices.

"Government health care agencies need to be able to centralize applications into a single location, so they can be accessed by multiple devices," Padin explained. "Consolidating the infrastructure, uploading patient data, then allowing secure access into those applications from anywhere is a huge requirement today. This will allow greater government health care efficiency, and enable users to work wherever they are on any device."

Citrix can help the federal as well as state and local governments move forward on the health care IT collaboration front by offering secure mobility solutions to access patient data anytime on any device. Citrix offers a full suite of solutions that can provide optimized health care web site access with NetScaler. Regional hospitals and facilities can reduce bandwidth cost while gaining optimized performance with Cloudbridge's SD-WAN technology. Delivering apps, desktop and mobile apps is easy with the Citrix Workspace Suite.

"Citrix has been driving health care solutions for the past several years for some of the largest customers in federal health care, and our mobility solutions deliver clinicians instant access to secure patient data helping to bridge the electronic health record gap to and from referring physicians," Padin said.

Citrix solutions for health care simplify security, protect intellectual property, ensure data privacy and help IT meet HIPAA compliance mandates without compromising productivity or ease of use for the public sector.

At the end of the day, Padin believes that Citrix solutions are all about putting the patient first.

"Every day there are hundreds of thousands of patients that take advantage of the government health care system. The government health care workers need reliable secure data access to ensure faster care," said Padin. "Every day they need reliable access to their applications which is possible through a Citrix system that allows them and the government to make sure that everything is efficient, effective, and secure end to end."

TREND #3

INTEROPERABILITY

The Healthcare Information and Management Systems Society (HIMSS) defines interoperability as "the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user."

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

The health care industry has been concerned with interoperability for more than a decade now. A 2006 American Health Information Management Association article states, "In one way or another, every healthcare information management story this year will relate to interoperability."

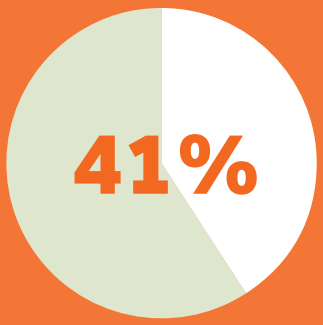
This trend has continued. As more government health IT initiatives — such as telehealth, population health management and precision medicine — require greater collaboration among patients, clinicians, providers and more, interoperability has become more important than ever.

More broadly, interoperability is key to the trifecta of U.S. health goals: improving health outcomes, improving health care quality and lowering health care costs. Achieving these goals requires a shift from an industry focused on institutional care delivery and health care providers to a "broad view of person-centered health."

ONC produced a nationwide roadmap to interoperability, which highlights how the shifting nature of modern health care requires greater communication among health care partners.

As community and home-based services gain a bigger role in health care and the industry takes the social determinants of health into greater account, interoperability is necessary to effectively communicate and implement information between new and old players in the health care field.

The government continues its outspoken interest in interoperability. At a conference in January 2016, CMS Acting Administrator Andy Slavitt said, "We are deadly serious about interoperability."



Only 41% of hospitals nationwide have electronic access to essential clinical information from outside sources when treating an individual.

78% of hospitals electronically sent a summary of care document

56% received one

[source]

INTEROPERABILITY IN GOVERNMENT TODAY

The process toward interoperability between the Defense Department (DoD) and VA has been an arduous one, and it is not complete yet.

As *Federal Computer Week* notes, both agencies serve 35 million patients. VA uses an in-house health IT system to manage its records, while DoD uses several systems to cover different needs. Having so many platforms and applications led to problems with coordinating and standardizing practices between the departments.

However, with the Joint Legacy Viewer, a web-based read-only interface, progress is being made. The program "combines information from about 300 record systems in real time to give clinicians and benefits administrators in both departments detailed patient histories on clinical interactions as far back as the early 1990s."

This is not a perfect solution, and more work needs to be done to include outside providers and non-electronic records. However, DoD and VA's focus on security and a high level of data exchange makes this program a strong example of what agencies can accomplish.

WHAT'S NEXT?

According to ONC's Shared Nationwide Interoperability Roadmap, by the end of 2017, a majority of health care providers should be using a common set of electronic clinical information at the nationwide level. This common set will include standardized data elements, such as demographics, so that organizations can better connect electronic health information across a variety of systems and platforms.

The roadmap also calls for a "learning health system" by 2024. This array of interoperable health IT products for individuals, care providers, communities and researchers will ideally result in lower health care costs through the identification and reduction of waste, improved population health, empowered health consumers, and greater technological innovation. This system will help achieve the three overarching aims of U.S. health care and involve patients more fully in their care.

Interoperability efforts must also address the growing sources of information and health records. People are increasingly using wearable tech and mobile applications that produce data. All this combined with the growing use of the social determinants of health means that interoperability efforts must be able to unite a broad array of information types, interfaces and sources.

WHAT YOU NEED TO KNOW

#1: Maintaining individual privacy and data security is key.

Many regulations govern health data, such as the Health Insurance Portability and Accountability Act and more general privacy laws. Organizations must have equivalent security standards so data will be protected as it moves from location to location.

#2: Many other trends rely on interoperability.

Interoperability is a desirable goal on its own, but added value comes from its role in other trends. To reap the benefits from population health management, precision medicine, telehealth and more, providers, patients and other care partners need to be able to share and access collective information.

#3: Interoperability builds patient engagement.

Not only will patients be able to see their entire health record as a cohesive narrative, they will also be able to produce their own health data to contribute to this record. This level of engagement will help the shift toward patient-focused care and improve the quality of care in the long run.

PUBLIC SECTOR SPOTLIGHT

DEALING WITH CHANGE IN FEDERAL HEALTH IT

An interview with Dr. B. Vindell Washington, Principal Deputy National Coordinator at ONC

Health IT is characterized by change. The current technology is a change from previous iterations; it changes the way patients and providers approach health care. These shifts can be challenging and they can be positive, but in both cases, they alter the industry. GovLoop talked to Dr. B. Vindell Washington, Principal Deputy National Coordinator at ONC, about the transformations he has seen in health IT and why they matter.

Washington noted that from the health care perspective, the government and the private sector face similar IT challenges. Both work to deliver care more efficiently based on technology and to have the right information available when it is needed. "The technology itself is really to further the end, and I think we're at our best when we're thinking in terms of whether or not technology is doing just that," Washington added.

Considering the interplay between the government and the private sector, ONC works to coordinate efforts across both sectors. "I think people recognized early on that you could end up with more waste than you expected if you didn't have some strategy for coordination across both the federal government agencies and the technology sector," Washington said. This perspective of coordination, without a financial or regulatory angle, allows the agency to bring together stakeholders from both sides to discuss best practices.

The need for best practices is especially important in light of the challenges of health IT implementation. Washington outlined two main obstacles. First is the adoption of new technologies. He likened it to his time in the Army and the early use of telemedicine. Because telemedicine required unfamiliar technology, he was forced to adapt his methods to accommodate it and learn how to effectively incorporate the new tools into his routine in order to provide the best possible care. A similar need for adoption, adaption and change management is present now as the industry faces new advances.

The second obstacle is the rapid growth of EMRs and the lack of interoperability. There are hundreds of different EMR providers, making easy information flow among them challenging. Few standards exist for information transmission, so to achieve interoperability, organizations need to develop common standards and then alter their data systems to align with those standards.

One of ONC's most important documents addresses this second challenge. "Connecting Health and Care for the Nation" is a nationwide roadmap to achieving interoperability in the next 10 years. The guide calls for a collaborative effort between public and private health care stakeholders to provide shared goals and guidelines for all members of the health care industry.

In addition to engaging with public and private partners, the roadmap also encourages security adherence by providing a clear understanding of what the relevant rules demand. By establishing common standards that are federally recognized, the roadmap will help bridge gaps between information systems.

At the end of the 10 years, Washington imagines a "learning health system," in which data is clearly available for health care partners, and they can use it to provide better care at a lower cost. "As providers get longitudinal records on patients and can see what has been successful and share that information, that actually makes for an advancement of medical care that we really just haven't had the opportunity for before," he said.

Washington is excited for the future. The majority of hospitals and physicians' offices use health IT and electronic records. This massive wave of digitization lets the government accomplish things that originally seemed years away. "If you think about things like the Vice President's [National] Cancer Moonshot, the payment delivery system reform, the President's Precision Medicine Initiative, none of these things are possible if the health care information was not digitized," he said. "So the most exciting thing is that we're at a point where we can really stand on that platform and reach for the stars."

This is where health IT's changes shine as a positive force. "I have twins that are in medical school right now, and it's been interesting to me that their life in medicine is going to look nothing like my life in medicine," he said. He learned fixed methods for treating high blood pressure, but his daughters are learning how to use precision medicine to target the treatments to a patient's genetic makeup.

Health IT will change how providers treat diseases like cancer and Parkinson's but also more common ailments, such as high blood pressure. It will change the health discussion to include more than just responses to illnesses or accidents by focusing on maintaining wellness. "I think that in the world that my daughters will inherit as providers and the world that we'll all live in as patients and consumers, we'll have the opportunity to have a lot more health deliverables and a lot happier times to come than I think any of us knew," he concluded.

TREND #4

DATA ANALYTICS

An IBM report defines data analytics as "the systematic use of data and related insights developed through applied analytical disciplines to drive fact-based decision making for planning, management, measurement and learning." Data analytics in health care uses the vast amounts of information available to produce actionable insights to improve health outcomes.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

All levels of government are facing complex challenges. Citizens are demanding greater engagement and more services, and governments must meet these demands with fewer resources. Data analytics offers a solution, allowing agencies and organizations to gain new insights.

This is especially important in health care. As costs rise, people expect more, and the government is placing greater demands in terms of accountability, governance and oversight.

The first U.S. Chief Data Scientist, D.J. Patil, agrees. He touted the benefits of analytics in government, saying, "In the case of health care, [there] is data that benefits everybody. If everyone is able to have a safe way to provide their data, we're going to be able to learn so much about the types of chronic conditions that are typically undiscovered."

Data analytics is key to other health IT trends, such as population health management and precision medicine. As government health care shifts to patient-focused care, data analytics is necessary to better understand how individuals and populations use health services, provide more targeted care and evaluate the impact of that care.

Health analytics is not limited to medical records. Information from a variety of sources, such as social services, education and geography, can help produce insights about population characteristics. For example, Indiana is using data analytics to identify causes for the state's high infant mortality rate in order to develop an effective response.

Based on the success of smaller projects, data-based opportunities are expected to shave 12 percent to 17 percent off the $2.6 trillion spent on health care in the United States.

[source]

ONLY 10 PERCENT

of health care professionals are using advanced data collection methods that have predictive data analytic capabilities

[source]

DATA ANALYTICS IN GOVERNMENT TODAY

Last year, the U.S. Drug Enforcement Administration announced that deaths from drug overdoses have surpassed deaths from car crashes and firearms each year since 2008.

A *Governing* article discusses how the Massachusetts Department of Public Health used data analytics to address this issue. Massachusetts is not the first state to use technology to mitigate overdose deaths; almost every state has a prescription drug monitoring system to collect and analyze electronic prescriptions to flag individuals who might be abusing prescription painkillers.

Although these programs have had some success, they have limits. They cannot track illicit drug use and require electronic prescriptions while more than 40 percent of prescriptions are on paper, for example. Massachusetts' analytics program, on the other hand, attempts to identify hotspots where possible overdoses and deaths might occur by spotting patterns in datasets, such as painkiller prescriptions and information on previous overdose deaths. The state can use these patterns to make more informed decisions about how and where to use resources.

WHAT'S NEXT?

There are challenges that the health care industry needs to overcome before data analytics can reach its full potential.

The article on Massachusetts' analytics program lists two: first, it can be challenging to connect and integrate data from different sources in a way that produces useful analysis and insights, and second, when real-time analysis is needed, the necessary computing software is expensive. Effective data analytics will require organizations, such as state Medicaid programs, to modernize their systems and interoperate with datasets from other organizations in addition to patient-generated information.

Prescriptive analytics will also become more important as agencies and organizations look to improve their services. Unlike predictive analytics, which shows a likely outcome, prescriptive analytics "demonstrate[s] suggested actions to make healthcare providers more successful, profitable, or responsive to patient needs." It can help identify areas of improvement in treatment, reduce the rate of readmitted patients and lower the cost of health care in general.

In addition, data analytics will be vital in precision medicine's success and the shift to value-based care, providing both with evidence-based results to promote more effective health services.

WHAT YOU NEED TO KNOW

#1: Successful data analytics relies on interoperability.

With more and more sources of health data, effective analysis needs to integrate information from a variety of datasets. If information is siloed away, the analysis will be incomplete and not produce the best possible insights.

#2: Predictive and prescriptive analysis will inform future decisions.

Agencies and organizations must be able to do more with less. Analytics will help allocate resources in the most effective fashion and provide insights as to how they can improve their services and reduce costs.

#3: Patient-generated data can help improve insights.

The wearable tech market is expected to grow in the next few years, providing new sources of patient-generated data for analytics. This and other social data will help produce a more complete picture of an individual's health.


No one knows
Hadoop
like Cloudera.
cloudera

INDUSTRY SPOTLIGHT

CLIMBING MOUNT EVEREST: ADVANCING PRECISION MEDICINE THROUGH TECHNOLOGY

An interview with Shawn Dolley, Industry Leader, Health and Life Science, Cloudera

Health IT, precision medicine, and genomics are a lot like climbing Mount Everest. Climbing the mountain the first time takes a lot of time, money, and other resources, but once the summit has been scaled, future climbers can work to make the process easier and achieve new goals that would have at one time seemed impossible.

Additionally, precision medicine and genomics once required a significant initial lift, but advances today in science and technology are making these approaches more common. Cloudera, a leader in big data management and analytics that has made a significant investment in President Obama's Precision Medicine Initiative, is helping make the climb even easier.

To understand more about precision medicine's climb up Everest, GovLoop spoke with Shawn Dolley, industry leader, Health and Life Science at Cloudera, about the progress genomics and precision medicine have made and what the future holds for the field.

One reason such advances in genomics are happening today is thanks, in large part, to advances in big data. Dolley said the first attempts to catalog a genome marked "the first shovel hitting the ground of the biggest dig of our lifetimes." Genetic sequencing has since become cheaper and faster, and much has changed from those initial sequencings, including updated biological methods of sequencing and greater innovation in how we understand genomic data. That innovation includes the development of bioinformatics, the use of technology to manage biological information.

One of the biggest challenges for bioinformaticians had been dealing with vast amounts of genomic data – the volume of genomic data is expected to reach two to four exabytes per year by 2025. However, the explosion of big data and the tools to handle and analyze it have made this obstacle more manageable and thus, laid the groundwork for the strides being made in precision medicine today.

While health IT may have the tools to handle big data now, health researchers don't always know how to implement these solutions. That's where Cloudera comes in. They've announced plans to train 1,000 precision medicine researchers in relevant big data and data science technologies and make significant investments in software, training, and services across fifty organizations over the next three years. With this move, Cloudera hopes to change the conversation about what is technically possible, what teams can afford with existing budgets, and how to collect, store, and analyze data. The goal, Dolley said, is to bring clinicians and researchers together, giving them an opportunity to share bodies of knowledge, foster collaborative innovation, and drive toward higher standards of care.

Though huge advances have been made in terms of the use and implementation of big data analytics for health IT, security remains a major concern for genomics and precision medicine because health data often contains personally identifiable information. HIPAA produced a framework and standards for security in the United States, and Cloudera seamlessly incorporates those standards into their technology suite. "Cloudera has made investments in a technology suite that can be turned on and configured to be HIPAA compliant without having to use any other tools," Dolley said. "IT folks in bioinformatics don't want to have to talk to other companies and fit a bunch of tools together." This native compatibility has helped Cloudera become dominant in the health IT sphere.

With all of these new technologies, precision medicine can change how we view healthcare. According to Dolley, signal detection – or deriving insights and patterns from data – is a "boots on the ground problem for the most part," as it is often difficult to get usable datasets at the ground level. However, researchers already have the tools needed to analyze the data. Once technology makes it easier to obtain usable datasets from all environments, researchers can begin to identify actionable insights based on the information.

Big data has ushered in a renaissance of clinical prediction. For example, hospitals can analyze patient data and understand why some patients are returning frequently. This type of predictive analysis can help them reduce cases of readmission by targeting care and resources. Similarly, as precision medicine gathers more genomic data, it builds a real-world evidence database for clinical trials and other research.

Dolley imagines a great future for genomics and precision medicine. "We're no longer really wondering how we're going to get a thousand people to the top of Everest; we know how we're going to do that," he said. "Now we're working on skiing down Everest and making it accessible to everyone." With further advances in analytics, technologies, and collaboration, the only thing we will need is to ask the right questions.

TREND #5

HEALTH DATA IN THE CLOUD

According to NIST, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. It's important to health today because more health organizations are moving their operations and data to the cloud for convenience and cost savings.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

A sobering fact: 90 percent of data today was produced in just two years. Additionally, nearly every day, about 2 quintillion bytes of data are generated. And the amount of data being produced, especially in the public sector, is growing exponentially. Because of this, more organizations — including those in the field of health care — badly need servers.

But instead of every organization owning and maintaining physical servers, which is not realistic, cloud computing — or storing data on remote servers, often owned by another organization that offers this as a service — has become a popular alternative. But is this safe for sensitive patient health data?

Additionally, according to a report by the Cloud Standards Customer Council, "compared to other industries, the healthcare industry has significantly underutilized technology to improve operational efficiency. Most healthcare systems still rely on paper medical records. Information that is digitized is typically not portable, inhibiting information sharing amongst the different healthcare actors. Around the globe, healthcare reform has mandated that it is time for healthcare information technology (HIT) to be modernized and cloud computing is at the center of this transformation."

So government health is at a turning point, of sorts, when it comes to cloud computing. More health information and patient data must be stored in the cloud for ease of access and interoperability issues. Additionally, there's this to consider: When it comes to health data, the more people who can get to it, the more valuable it is — and more people can get to that health data if it is stored in the cloud. This leads to great developments in health care — health organizations can use cloud technology and related tools to give researchers an unprecedented ability to access and mine health data.

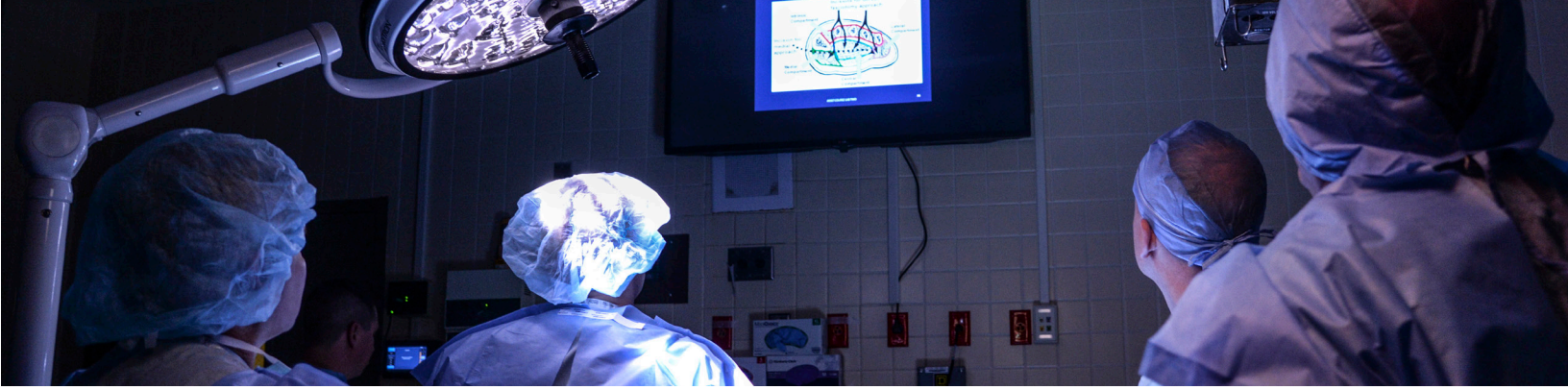
But how can government ensure that sensitive patient and health data is secure and remains private in the cloud? These are the opportunities and challenges that government is presented with when moving health data and information to the cloud.

U.S. federal spending on **private cloud** will be

$1.7 BILLION

vs. just ***$118.3 million*** on **public cloud**

[source]



HEALTH & CLOUD IN GOVERNMENT TODAY

When it comes to the cloud, agencies have several options. Some choose to create a private cloud, where they own all the hosting services. Some go to an external vendor. Some create a hybrid cloud model. Michigan and Illinois are proving that when it comes to health IT, a partnership may be the way to go.

In late 2015, the Michigan Department of Health and Human Services (MDHHS) worked with the state of Illinois, the Michigan Department of Technology, the federal Office of Management and Budget, and a private vendor to launch the second phase of the nation's first completely automated real-time and cloud-enabled Medicaid system.

"Moving to the cloud allows us to better serve our residents and improve health care delivery, all while reducing costs," MDHHS Director Nick Lyon said in a press release. "This unique initiative enhances our ability to maintain Medicaid systems, meet state and federal guidelines, and work with partners such as Illinois to create a multi-state platform that can meet the specific needs of our residents."

Now that both states' Medicaid systems are in the cloud, better fraud detection is possible because more people can access and review data, and the two states share one infrastructure, which has reduced operating costs for both.

WHAT'S NEXT?

Cloud computing for health will in no way slow down — the need for health data, ease of access and interoperability will demand that health information, data and platforms move to the cloud. And because this data is more sensitive than other data types moved to the cloud, health care organizations must make sure to develop, maintain and optimize security processes for all cloud environments, perhaps even more so than in a traditional data center model.

But the outlook for cloud computing for health care agencies is overall rosy. HealthCare.gov moved its systems to the cloud with great success, inspiring other federal agencies to move from antiquated IT systems to the cloud for ease of use, better performance and security.

WHAT YOU NEED TO KNOW

#1: Security will remain paramount.

A health information breach affected 111,812,172 individuals in 2015. So it's important to remember that not all cloud providers are created alike. Risks need to be managed and operational integrity, plus data security, must be maintained.

#2: Cloud computing will continue to be important not just for the ease of use, but for research purposes.

FDA recently announced the launch of precisionFDA, a cloud platform that will "supply an environment where the community can test, pilot, and validate new approaches" to next-generation sequencing tests.

#3: The hybrid cloud model is growing in popularity for health agencies.

Hybrid cloud adoption is set to triple in the next three years in the public sector, and several government agencies, including HHS, are pursuing hybrid cloud strategies.

TREND #6

POPULATION HEALTH MANAGEMENT

Population health management has become a popular phrase in the past decade, but there is little agreement on a definition. In general, it is a patient-focused strategy of understanding and addressing the overall health needs of a group to improve outcomes and manage their care to reduce costs. This includes consideration of measures of health other than illness, such as overall wellness.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

The Institute for Healthcare Improvement (IHI) established the Triple Aim Initiative in 2007 as a framework for optimizing the health care system. The three parts of this initiative are improving the patient experience of care, reducing the per capita cost of health care and improving the health of populations.

HHS has adopted this tripartite system as part of its National Quality Strategy, emphasizing the widespread influence of IHI's initiative. One of the strategy's goals builds on IHI's focus on population health: "Improve the health of the U.S. population by supporting proven interventions to address behavioral, social, and environmental determinants of health in addition to delivering higher-quality care."

In addition, population health management is key to value-based care, one of the goals of the Affordable Care Act. HHS aims to have 30 percent of Medicare payments moved to value-based systems by the end of 2016 and 50 percent by 2018. The existing payment system is fee-for-service, in which providers are paid based on the number of visits and tests they order; in a value-based system, they will be paid based on the value and outcome of the care they deliver. HHS' ultimate goal for the payment model relies on population health management as an indicator that medical care provides value for the members of a community.

CMS also connects population health with more effective health care, listing prevention and population health as one of its four main goals. The whole-person and community approach of population health helps providers and clinicians understand how groups of people use health services so that they can deliver more effective care.

The difference in cost of care for a well-managed and understood population vs. a loosely managed population of 5,000 people can exceed **$10,000,000** per year.

[source]

95%

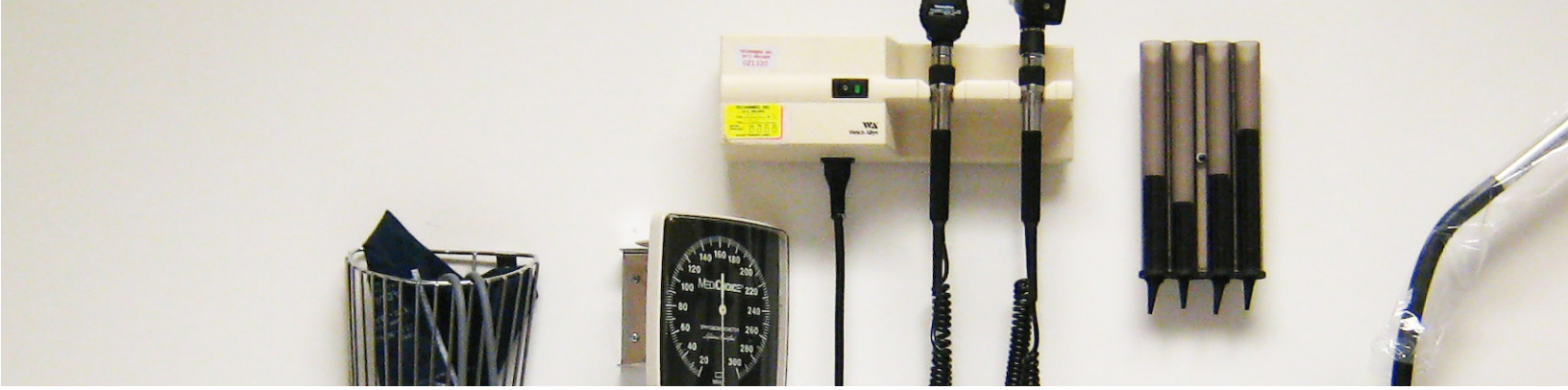
of U.S. health care spending is for direct medical services, but access to quality medical care prevents only

10%

of avoidable deaths.

The rest is connected to nonmedical indicators, such as social circumstance and behavioral patterns.

[source]



POPULATION HEALTH IN GOVERNMENT TODAY

Seeing the big picture helps save money.

Colorado's primary health care program, the Accountable Care Collaborative (ACC), combines a fee-for-service payment model with value-based rewards to achieve its goals of improving member health, improving member and provider experience, and containing costs. The program uses regional care collaborative organizations (RCCOs) to create a network of primary care medical providers (PCMPs).

The network of providers can track health data through a statewide data and analytics contractor to identify patterns in how members use health care services, such as which areas use a higher proportion of services and which services are used most frequently.

A report by 3M discusses how this program uses metrics to institute a value-based incentive system: "The RCCOs and PCMPs can also track key metrics such as emergency room visits [and] hospital readmissions.... This ability helps them manage the value-based payment component of the ACC, which grants them incentive payments when they meet or exceed targets in these areas." Through this model, ACC achieved about $100 million in gross medical cost savings.

WHAT'S NEXT?

Population health management is based on the idea of having the right information for the right population at the right time. However, to fully realize population health management's potential, clinicians, providers and patients need to change how they approach health care.

EHRs are key for effective population health management. Medical care providers need to be able to collect and share information about patients on a regular basis. Primary care providers, hospital doctors and specialists need to be able to share patient records and data to provide the big-picture perspective necessary for population health.

Although EHRs are common now, they often do not have the capability to process the required information. EHRs and health information systems must advance to the point where they can receive and aggregate data from a variety of sources, analyze the data to produce actionable insights, and offer a centralized point of access for all relevant health care professionals. Greater interoperability and advanced data analytics will provide the health care industry with stronger management of population health.

WHAT YOU NEED TO KNOW

#1: Greater interoperability is necessary.

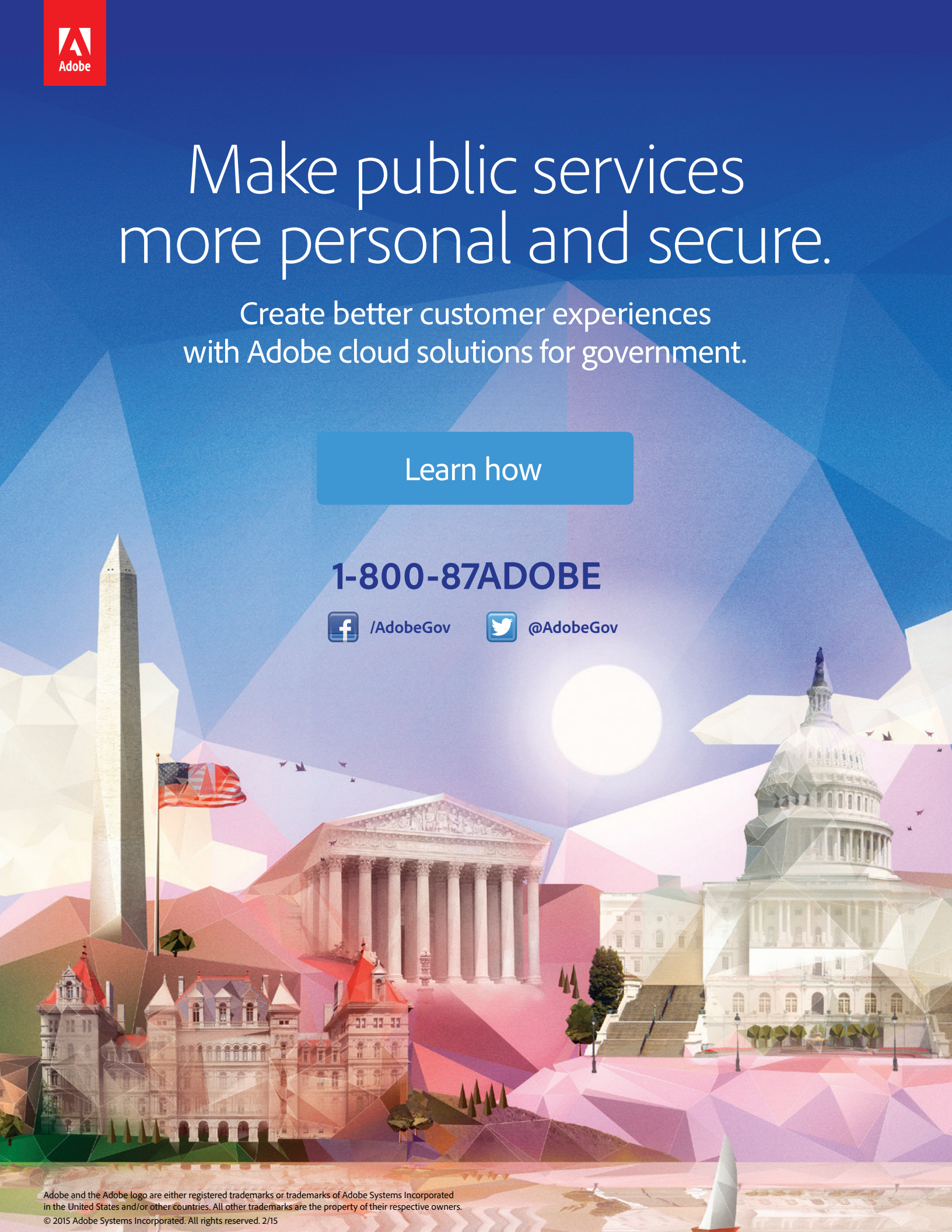
Population health relies on a big-picture understanding of an individual's and a community's health. Complete record integration is an essential stepping stone for community care, and population health growth depends on providers' ability to share and use information.

#2: Patient-centered care will use vast amounts of data.

To understand how populations are using health services and how to best treat them, providers will need to identify the at-risk populations and measure their service usage. This will require collecting vast amounts of data and analyzing it to produce actionable insights.

#3: This is essential for the shift to value-based care from fee-for-service care.

As more health care providers switch to a value-based payment model as per HHS' requirements, clinicians and providers will turn to population health management as a metric for the quality and outcome of the care.



Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.
© 2015 Adobe Systems Incorporated. All rights reserved. 2/15

INDUSTRY SPOTLIGHT

DATA-CENTRIC SECURITY FOR SELF-SERVICE AGENCIES

An interview with Kumar Rachuri, Director of State and Local Government Solutions, and Steve Gottwals, Technical Director of Security, Adobe Systems Federal

As digital transformation continues to push government services and citizen interactions online, safeguarding content and data in a landscape filled with laptops and mobile devices is a new challenge. Recent federal information security policy guidelines are recognizing this threat and influencing how state and health agencies should address these data security concerns moving forward. As a part of comprehensive cybersecurity plan, agencies should adopt multiple, dynamic protections that travel with data wherever it goes.

A key element to any multi-layered cybersecurity strategy is data-centric security, which consists of protecting the native file format itself. This helps ensure that data remains secure wherever it travels or is stored. To learn more about data-centric security, GovLoop spoke with Adobe's Kumar Rachuri, Director of State and Local Government Solutions, and Steve Gottwals, Technical Director of Security, to see why health agencies and departments need to think about adapting a data-centric approach for the self-service systems they deploy.

Rachuri explained the current landscape of self-service portals deployed at the state and local government level or in health agencies and departments. "For organizations with external-facing services, self-service portals and online forms are a key part of user interactions," he said. "In today's government environment, online interactions are increasingly common. Many organizations have successfully extended paper-based forms processes to online digital forms and self-service portals, whether internal or external-facing."

However, this initial success in moving to digital services has created a new set of potential concerns. As the breadth of online services expands, how can health departments and organizations effectively create, publish, track, manage, and secure their and their users' sensitive data?

"A dynamic, data-centric approach is a new best practice that is being driven by federal cybersecurity policies and standards that have an impact on health and human services data, particularly personally identifiable information (PII)," said Gottwals. He also pointed out that a strong federal-state partnership in defending government networks is aided by cybersecurity tools and resources available to state governments through the General Services Administration (GSA) Continuous Diagnostics & Mitigation (CDM) Blanket Purchase Agreement. CDM is a dynamic approach to fortifying the cybersecurity of government networks and systems.

"With data-centric security, no matter where the data goes, it carries protection" Gottwals explained. Data-centric security targets and uses technology to help protect the data itself, regardless of its location—inside or outside the firewall and on any device. It adds another critical layer of fortification to existing security measures. "It also encrypts the native file format itself," he said. "This helps ensure data remains more secure wherever it travels or is stored."

This is important, Rachuri said, because it addresses the issue of data that's not just static, but from when it is created. "Oftentimes, government can overlook the security of the data once it's in motion," he said. "If you think about any information you gather from a data perspective, what do you do with it? You put it in a document, or you put it in an email, and then you send it out to people. You communicate that information out to providers or the doctor's office. The data is always in motion. It doesn't just sit in a datacenter."

To implement this across a government organization it is important to implement three key criteria:

1. An ability to remotely deliver dynamic policy and access changes on the fly without having to revoke and renew document access.
2. Continuous auditing and reporting, regardless of location.
3. Use of digital signatures to confirm the identity of each person or organization who signed a document, and that it hasn't been altered in transit to help ensure authenticity and integrity.

Adobe has been helping customers protect sensitive data and documents for over two decades, and today they continue to do so through robust digital rights management (DRM) combined with real-time data analytics that provide a powerful audit trail on document interactions.

With Adobe digital rights management solutions, "Organizations are adding an extra level of protection at the data layer, beyond their existing network and device mitigations," Gottwals said. "It's the data itself that gets encrypted, so it continues to help protect documents independent of storage or transport."

TREND #7

TELEHEALTH

The Health Resources Services Administration defines telehealth as the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health, and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

Doctors are using iPads to record information instead of scribbling notes on a paper pad. Nurses are browsing through EMRs instead of file drawers. Hospitals are adopting the cloud to store patient data and make it accessible to care providers anytime, anywhere.

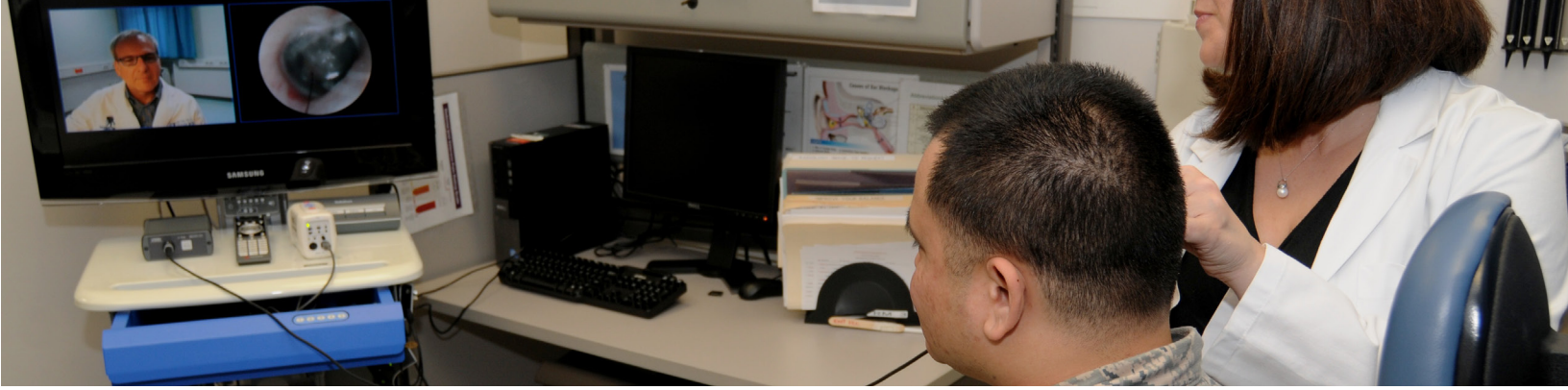
Technology has completely transformed the entire field of health care in the past two decades, and the results have vastly altered the manner in which patients and health care professionals manage patients' well-being. As health care continues to turn to technology to deliver more effective treatments, the practice of telehealth is starting to take center stage. Telehealth helps meets citizens' demands and needs for mobility, flexibility and faster care.

Today, demand for telehealth services such as video communications and remote patient monitoring is rapidly increasing because networks and infrastructure are better able to support it. Additionally, as rural care demands increase, and as agencies such as the Indian Health Service and VA need to deliver services to larger groups of patients, telehealth is being used more than ever. In fact, market research firm IHS predicted in a December 2013 study that the U.S. telehealth market will grow from $240 million in 2013 to $1.9 billion in 2018.

The telehealth market is clearly poised to explode, and more agencies and health care organizations are looking for guidance on how to best use these technologies.

VA telehealth services are growing at a rate of 22% per year.

[source]



TELEHEALTH IN GOVERNMENT TODAY

Even astronauts get sick.

That's the reason NASA, and those on the International Space Station, are turning to telehealth practices. The ways in which they are using telehealth and overcoming some of the challenges can pave the way for how telehealth technology should be deployed in rural or low-income areas nation- and worldwide.

NASA has reduced the risk of medical emergencies on the space station by training the crew in telehealth methods and telemedicine consultation. As this *Government Health IT* article explains, "NASA has mitigated the risk of medical emergencies aboard the space station by training the crew medical officer and by using on-board ultrasound and an Earth-based telemedicine consultation. Space flight, though, presents several challenges, such as engineering and space constraints, limited bandwidth for data transmission, a lack of advanced diagnostic equipment and the absence of a physician. How space station crewmembers overcome these challenges may present a model to Earth-bound programs."

These challenges of data lag, imaging transfers and slow connections can teach lessons and eventually help those implementing telehealth technology on Earth in rural areas where they face these same data and transfer issues.

WHAT'S NEXT?

The growing adoption of telehealth in government is likely to continue, as the National Center for Policy Analysis (NCPA) explained in a recent report.

In the past two years, 25 states have revised their professional standards and licensure requirements to accommodate providers offering health services via telemedicine. Additionally, CMS changed its fee schedule in 2014 to encourage more telehealth practices. Moreover, NCPA's report states that the number of patients using telehealth services is expected to reach 7 million by 2018, up from 350,000 in 2013.

But this massive growth comes with challenges. All levels of government will have to watch out for security concerns, state licensure laws and support for technology infrastructure as they work to implement more telehealth.

WHAT YOU NEED TO KNOW

#1: Telehealth will be critical in the coming years to reach underserved populations.

Those who live far from medical centers or who find it difficult to travel will most benefit from telehealth. VA telehealth services are growing at a rate of 22 percent per year, and telehealth is also growing as a means of treating prisoners remotely.

#2: Interoperability will remain an issue for telehealth.

There is no industrywide standardization for telehealth technology and services, and many outside organizations have different security requirements or technology standards, which can make it difficult to operate on the same platform.

#3: Despite challenges, this is an exploding market.

At the moment, there are 1.25 billion in-person care visits every year to physicians' offices, emergency rooms and outpatient clinics, according to CDC. A recent marketing analysis states that eventually, virtual medicine could handle 417 million of those.

PUBLIC SECTOR SPOTLIGHT

UNIFYING HEALTH & HUMAN SERVICES IN CALIFORNIA

An interview with Scott Christman, Acting Agency Information Officer for the California Health and Human Services Agency

The California Health and Human Services Agency (CHHS) is a massive organization, spanning 12 departments of varying sizes, 33,000 workers, and running over 200 public health programs. Coordinating health efforts across an organization of that size brings several challenges, but California has worked to overcome departmental mission and data silos to move toward unified agency.

Scott Christman is the Chief Information Officer at the Office of Statewide Health Planning and Development, one of CHHS' departments, and the Acting Agency Information Officer for CHHS overall. He talked to GovLoop about the strategies CHHS used to create a unified agency, challenges faced, and trends he sees for the future.

Traditionally, Christman said, the 12 departments "focused on their individual programmatic missions," creating data silos. In addition, "[CHHS has] a very large Medicaid program, we have a full range of social and human services delivery; all things that you would expect from a health and human services organization are included in the portfolio." CHHS also partners with counties as well as the federal government. This means CHHS had to deal with several individual strategies and governance plans throughout the departments, programs, and civil partners.

However, CHHS is shifting from a programmatic focus on healthcare to a whole-person view and person-centered care. This new focus requires more collaboration among the separate departments, so CHHS now views their agency as a single unit with a portfolio of 12 different departments. The departments coordinate their efforts in order to serve the broader agency. Christman offered an example of this new focus: "If we need identity and access management functionality, ideally we can leverage a shared service that would deal with identity and access management for any CHHS program, as opposed to individual programs developing their own functionality."

This movement to shared investments across the agency is most clearly manifest in the governance structure. Christman noted, "We've created a horizontal agencywide cross-cutting governance structure that has representation from the 12 departments. This is a structure that's sponsored by the Secretary and Undersecretary [of CHHS], and it's allowed us to begin thinking about leveraging investments across departments and focusing on shared services that can provide a functionality that many programs benefit from."

The departmental input and high-level support are key aspects of the structure's success so far. When asked what tips he had for other agencies attempting a similar project, he recommended creating a short, simple, focused strategy. Decide what is

important for your agency, develop your strategy around that, and don't let the plan just sit on the shelf. He also emphasized the importance of strong leadership and a high-level champion for the plan, as well as reinforcing a core message to help shift organizational cultures.

In terms of cultural shifts, CHHS' open data project, the first agency-wide initiative, has been a major success. Christman said, "It's greatly improved accessibility to data. We can have better informed conversations, and it can drive more informed work in communities. But it also helps us internally and advances our interest in data sharing. We aren't doing Medicaid open data and public health open data; we're doing Health and Human Services open data." This shift matches the agency's new focus on person-centered care and design, allowing users to identify relevant information without having to delve into departmental divisions.

Christman acknowledges that there are still challenges. One of the biggest challenges is the variation in departmental size. The Department of State Hospitals has 11,000 employees in hospitals across the state, while the smallest department has around 80 people. The differences in departmental capacity and resources make it difficult to standardize initiatives across the agency. Another challenge is the lack of a developed data science employment pool for state government, making it difficult to recruit new staff to aid in the initiative.

Cloud provides a solution for some of those challenges, providing scalable capacity and a collaboration platform throughout the agency. Christman said, "We want to focus our resources on our core competency, and we want to focus more on the development of data assets, for both public and internal use. Managing physical infrastructure is just not one of our core competencies. The resources spent on that management could be used instead for critical agency initiatives." This includes using data to solve problems and improve agency programs and services.

Looking ahead, the future for CHHS will continue the focus on development of data assets and building a culture of using data to improve operations and services. In order to match the idea that CHHS is one agency, Christman said, "We should be able to move data between departments in order to put the data together, provide better analytics, and drive better programs, better service delivery, and better outcomes." These steps and constant progress will help unify an extremely diverse system, which means better care for California residents in the end.

TREND #8

PRECISION MEDICINE

The National Institutes of Health defines precision medicine as "an emerging approach for disease treatment and prevention that takes into account individual variability in genes, environment, and lifestyle for each person." This information can give researchers and clinicians greater insight into a disease and how it can be treated.

WHY THIS TREND MATTERS IN GOVERNMENT RIGHT NOW

In his 2015 State of the Union address, President Barack Obama announced the creation of the Precision Medicine Initiative (PMI). This initiative capitalizes on the convergence of several factors: broader adoption of EHRs, greater patient engagement in health research, more mobile health technologies, more sophisticated data analytics and less expensive genomic analysis.

These factors mean that health care can shift from the traditional one-size-fits-all model in which doctors treat patients as if they were genetically identical, without any regard for differences in the disease makeup or individual responses. This can result in less effective and costlier treatments.

Precision medicine has already had some success, especially in oncology. Patients with certain types of cancer, such as breast cancer, melanoma and leukemia, can have their genomes profiled in order to provide physicians with a better understanding of their genetic makeup as well as the tumor's.

PMI aims to expand on these advances and spread its success to other common diseases, such as diabetes, heart disease, Alzheimer's disease, obesity and mental illnesses. In addition to helping target diseases, precision medicine will help provide insights into how we can increase overall population health and lower health care costs.

The initiative includes a $215 million budget to develop a national research cohort of 1 million volunteers, increase efforts to identify genomic drivers in cancer, build high-quality databases to make the data accessible and create interoperability standards to securely share data across systems.

*Sequencing the genomes of the about **1.65 million people** who will be diagnosed with cancer this year will produce*

4 BILLION GIGABYTES OF DATA

400,000 times all the information in the Library of Congress

[source]

PRECISION MEDICINE IN GOVERNMENT TODAY

While transformative, Obama's initiative isn't the first major effort in the field.

The Veterans Health Administration established the Million Veteran Project in 2012. The project aims to collect health information and DNA analysis from 1 million veterans and active-duty personnel. A *Military Times* article highlights the vast scale of the project, which currently has blood samples and medical histories from more than 455,000 veterans. VA officials expect to have more than 500,000 volunteers by June 2016 and reach the million-member mark by 2020.

The project reaches nationwide, with more than 50 volunteer sites, but also has centralized hubs for data sharing and sample storage. In addition to collecting information and blood samples, it has specialized ongoing research on the genetic makeup of individuals with schizophrenia, bipolar disorder, heart disease, kidney disease and substance abuse. *Scientific American* notes, "Now, as other research groups try to scale up their own efforts for the president's initiative, the VA effort is one of the lone guideposts in a field with few landmarks."

WHAT'S NEXT?

Included in PMI's budget is $130 million dedicated to the development of a volunteer research cohort through NIH. The agency funded a pilot program for a PMI Cohort Program informational website and participant interface, and enrollment is expected to begin later this year.

Armed with new genetic information and funding, the National Cancer Institute will develop new clinical trials on targeted cancer treatments and drug resistance, new laboratory research models, and a national cancer knowledge system to share new insights.

Precision medicine also changes the way patients interact with their health care. Although there is an emphasis on genetic makeup, precision medicine also looks more broadly at an individual's environment and lifestyle to provide the best possible care. This will require massive amounts of patient-generated data, leading to the increased use of mobile health applications. In turn, EHRs will need to be able to incorporate that data, requiring interoperability between the applications and the health records.

With so much personal data, security, analytics and interoperability are key issues that need to be addressed. NIH is working to develop effective methods for data sharing and analytics as part of the cohort program.

WHAT YOU NEED TO KNOW

#1: Security and privacy are major concerns.

As precision medicine initiatives gather the personal health data of hundreds of thousands of individuals, security needs to be balanced with effective data sharing. Researchers, clinicians and patients need to be able to produce, access and share data while protecting individual privacy and security.

#2: Data must be available and accessible.

Precision medicine needs to address problems of scale, incompatible technologies across hospitals and research centers, and data silos due to competition.

#3: Patient engagement is key.

PMI's success requires the participation and continuous engagement of a million or more Americans. For the cohort to be representative, the initiative must attract volunteers from a variety of age groups, health statuses, and geographic, social, and economic backgrounds.

MEET NEW HEALTHCARE CHALLENGES HEAD ON

What if doctors could improve follow-up care, monitor diseases like diabetes, schedule follow-up appointments and ping patients remotely to let them know the next steps they need to take to improve their care, all with an easy-to-use mobile app?

That would be revolutionary for patients and doctors.

The digital intelligence of the healthcare community has never been greater. That's why Red Hat is investing in the future of healthcare mobile application development.

LEARN MORE AT HTTP://RED.HT/1T2DM2A

DLT

redhat.

ABOUT & ACKNOWLEDGMENTS

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

THANK YOU

Thank you to Adobe, Citrix, Cloudera, DLT Solutions, Information Builders and Red Hat for their support of this valuable resource for public-sector professionals.

AUTHORS

Catherine Andrews, Director of Content
Sonia Chakrabarty, Editorial Fellow

DESIGNER

Kaitlyn Baker, Graphic Designer

PHOTO CREDIT

All photos licensed for use under Creative Commons 2.0.

Andrew Malone, Army Medicine, California Public Health, Charles Williams, Intel Free Press and Phalinn Ooi.

1152 15th St. NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop