Healthcare in the Digital World

Andy Wilson, M.D.
Vice President of Medical Affairs
Northern Dutchess Hospital

Today's Agenda

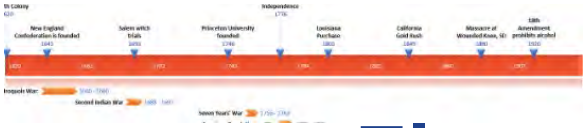
1. Introduction: Digital Medicine
2. Why is there no National Healthcare Portal?
3. Patient Portal Access
4. Security and Privacy Risks
5. Future of Digital Healthcare

History of Electronic Health Records

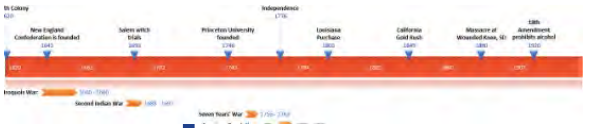
- **1960s-1970s**: The early development of electronic health records began in the 1960s, with institutions like the Mayo Clinic and Massachusetts General Hospital leading the way
  - Early systems were limited to basic data storage and lacked interconnectivity between departments.

- **1980s-1990s**: Advent of personal computing: hospital systems began adopting more advanced EHRs.
  - Development of VistA (Veterans Health Information Systems and Technology Architecture)

- **2000s**: The Institute of Medicine's 2001 report, "Crossing the Quality Chasm," emphasized the need for electronic records to improve the safety and quality of healthcare
  - Adoption of EHRs began to grow, but barriers such as cost and technical challenges slowed widespread implementation.



History of Electronic Health Records



- **2009 (HITECH Act)**: The Health Information Technology for Economic and Clinical Health (HITECH) Act
  - It provided $19 billion in incentives to healthcare providers

- **2010s-Present**: As a result by 2017 over 96% of hospitals had adopted EHR systems.
  - The goal of interoperability—allowing systems to communicate and share data effectively—remains a work in progress

- **2010s-Present**: By 2018, nearly all pharmacies in the U.S. had implemented e-prescribing.

- **2020-Present (COVID-19 Pandemic)**: The COVID-19 pandemic led to an unprecedented surge in telemedicine use. Regulatory changes, such as the relaxation of HIPAA regulations for telehealth and increased Medicare and Medicaid reimbursement for telemedicine services

National Healthcare Portal???

There is **no unified national healthcare portal** in the U.S. for sharing all Americans' health information due to several factors, including:

1. **Decentralized Healthcare System**: The U.S. healthcare system is highly fragmented, with different private and public insurers, health systems, and technology platforms. This makes it difficult to centralize health data.

2. **Privacy and Security Concerns**: Healthcare data is highly sensitive, and there are strict regulations, like the **Health Insurance Portability and Accountability Act (HIPAA)**, to protect patient privacy. A national health information system would need to balance data accessibility with privacy safeguards.

National Healthcare Portal???

3. **Interoperability Challenges**: Many electronic health record (EHR) systems are not designed to communicate seamlessly with each other. While efforts like **interoperability rules** under the **21st Century Cures Act** are trying to address this, creating a fully integrated system remains complex due to different data standards and technological incompatibilities.

4. **Political and Regulatory Landscape**: Healthcare is heavily influenced by political decisions, and there are varying opinions on how much the government should be involved in managing or centralizing healthcare data.

National Healthcare Portal???

5. **Political and Regulatory Landscape**: Healthcare is heavily influenced by political decisions, and there are varying opinions on how much the government should be involved in managing or centralizing healthcare data.
6. **State-Level Autonomy**: States manage healthcare data systems in varying ways, and federalism often leads to different approaches in terms of regulation and implementation.

Although there is no national portal, initiatives such as the **Trusted Exchange Framework and Common Agreement (TEFCA)**, which aims to create a network for health information exchange across the U.S.

Trivia:

Question:
Which of the following innovations in the digital age marked the beginning of widespread adoption of electronic health records (EHRs) in the U.S., and what federal initiative accelerated this transition?

A) The passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996, which created standards for electronic data exchange.
B) The introduction of the Affordable Care Act (ACA) in 2010, which mandated hospitals to adopt EHR systems for reimbursement eligibility.
C) The implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, which incentivized the adoption of EHRs.
D) The establishment of the National Health Information Network (NHIN) in 2004, which provided the first government-sponsored framework for digital health records.

Telemedicine

- The rise of **telemedicine** has made it possible for patients, especially older adults, to access healthcare from the comfort of their homes.
  - During the COVID-19 pandemic, the use of telehealth surged as it became a safer option for both providers and patients.

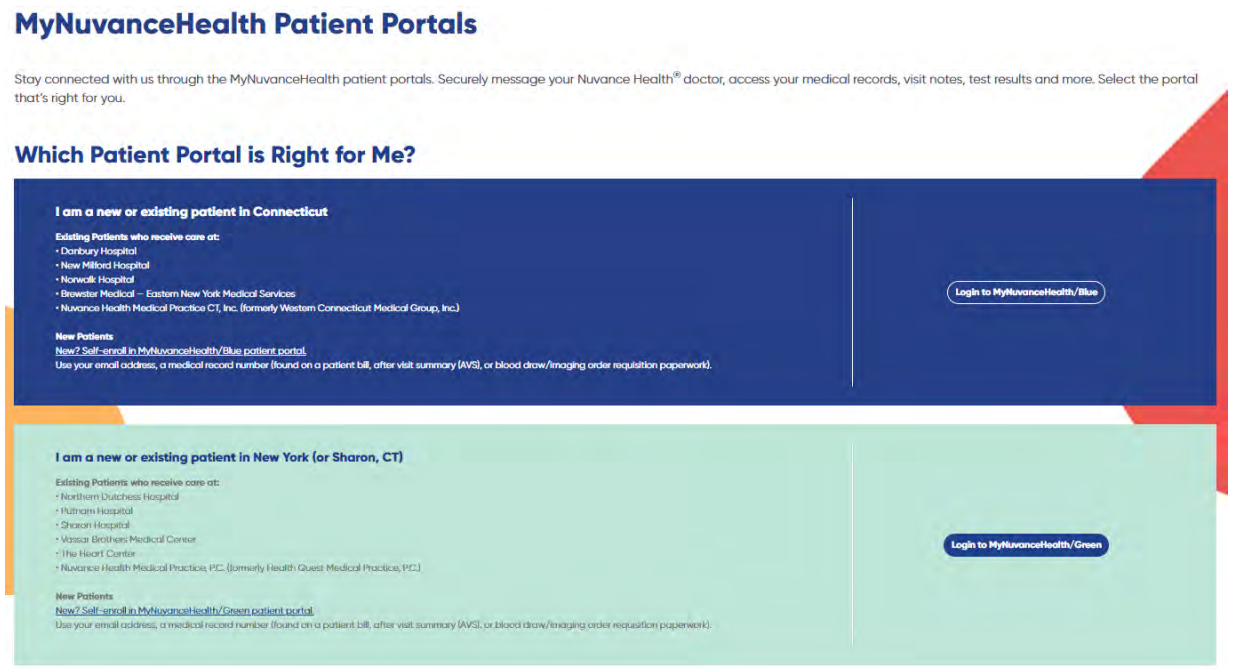
- Many older adults have:
  1. mobility issues or chronic conditions that make frequent doctor visits difficult. Telemedicine reduces the need for travel and provides convenient care for this demographic.
  2. Virtual appointments allow patients to consult with their healthcare providers via video calls, access prescriptions online, and manage their care remotely.

Telemedicine

- Virtual Waiting room
- Dialog to get appropriate history
- Explain results and diagnosis

Nuvance Health
Patient Portal

- Access to online records/communication
- Game changer for many people who have the ability to navigate



MyNuvanceHealth Patient Portals

Stay connected with us through the MyNuvanceHealth patient portals. Securely message your Nuvance Health® doctor, access your medical records, visit notes, test results and more. Select the portal that's right for you.

Which Patient Portal is Right for Me?

I am a new or existing patient in Connecticut

Existing Patients who receive care at:
- Danbury Hospital
- New Milford Hospital
- Norwalk Hospital
- Brewster Medical – Eastern New York Medical Services
- Nuvance Health Medical Practice CT, Inc. (formerly Western Connecticut Medical Group, Inc.)

New Patients
New? Self-enroll in MyNuvanceHealth/Blue patient portal.
Use your email address, a medical record number (found on a patient bill, after visit summary (AVS), or blood draw/imaging order requisition paperwork).

Login to MyNuvanceHealth/Blue

I am a new or existing patient in New York (or Sharon, CT)

Existing Patients who receive care at:
- Northern Dutchess Hospital
- Putnam Hospital
- Sharon Hospital
- Vassar Brothers Medical Center
- The Heart Center
- Nuvance Health Medical Practice, P.C. (formerly Health Quest Medical Practice, P.C.)

New Patients
New? Self-enroll in MyNuvanceHealth/Green patient portal.
Use your email address, a medical record number (found on a patient bill, after visit summary (AVS), or blood draw/imaging order requisition paperwork).

Login to MyNuvanceHealth/Green

Nuvance Health
Patient Portal

mynuvancehealth/green

Cyber Security Risks

1. **Hacking**: Target healthcare systems due to the sensitive nature of patient information
   - Example: 2020 **Universal Health Services** (UHS) Ransomware Attack:
     - Incident: One of the most notable attacks in 2020 occurred at ***Universal Health Services*** (UHS), one of the largest healthcare providers in the U.S. The Ryuk ransomware attack crippled its IT systems across hundreds of hospitals for weeks, affecting patient care, lab results, and scheduling. Staff had to revert to manual processes, which disrupted normal operations.
     - Impact: It was estimated that UHS lost $67 million due to the attack, which also led to delays in treatment for patients, including critical care.

Cyber Security Risks

- **Scripps Health Ransomware Attack** (2021):
  - Incident: In May 2021, Scripps Health, a prominent healthcare system in Southern California, suffered a ransomware attack that forced the hospital to take its IT systems offline. The attack led to delays in care, forcing the diversion of trauma patients and disabling access to electronic health records (EHRs).
  - Impact: The attack disrupted operations across four hospitals and impacted approximately 147,000 patients. The financial losses were reported to be over $100 million, including lost revenue, investigation costs, and recovery efforts.

Cyber Security Risks

- October 2023, **HealthAlliance of the Hudson Valley**, which includes Kingston and Margaretville Hospitals, experienced a significant ransomware attack.
  - The breach compromised patient data, including sensitive information like names, Social Security numbers, birth dates, medical records, diagnoses, lab results, medications, and insurance details.
  - The attack occurred over a two-month period from August 18 to October 13, 2023, before being discovered on October 12.
  - Once the attack was identified, HealthAlliance acted quickly to secure systems, notify law enforcement, and engage a third-party cybersecurity firm to investigate the scope of the breach.
  - This SHUT DOWN the hospital for several days.

Cyber Security Risks

- **Phishing Scams**: Cybercriminals may send emails or messages disguised as legitimate communications from healthcare providers or insurers, attempting to trick individuals into sharing personal information.
- This can lead to identity theft or unauthorized access to health accounts.
  - Example: A patient might receive an email claiming to be from their healthcare provider asking them to log into their patient portal, but it redirects them to a fraudulent site.

Cyber Security Mitigation

Mitigation Strategies

- **Use Strong, Unique Passwords**: Passwords should be complex and unique to each account.

- **Enable Two-Factor Authentication (2FA)**: Two-factor authentication adds an extra layer of security by requiring a second form of verification (e.g., a code sent to your phone) in addition to your password.

- **Be Cautious with Personal Information**: Be mindful of where and with whom you share personal health information. Avoid sharing sensitive data over unsecured networks (e.g., public Wi-Fi) and be wary of unsolicited emails asking for personal information.

- **Regularly Monitor Accounts**: Patients should regularly check their digital healthcare accounts and bank statements for any suspicious activity or unauthorized access to their information.

Nuvance Health's Role in Protecting Patient Data Encryption:

- Nuvance Health employs **encryption protocols** to protect patient data in transit and at rest. This ensures that even if data is intercepted, it cannot be read

- **Regular Security Updates**: The hospital's IT infrastructure is regularly updated with security patches and system upgrades to defend against emerging cyber threats. This includes updating software, monitoring networks for vulnerabilities, and using advanced firewalls.

- **Training and Awareness**: Nuvance Health also prioritizes staff training on data security protocols, including recognizing phishing attempts, safeguarding patient information, and adhering to privacy regulations like HIPAA (Health Insurance Portability and Accountability Act).

Nuvance Health's Role in Protecting Patient Data Encryption:

In the context of healthcare cybersecurity, which of the following best describes a "zero trust" security model, and why is it increasingly critical for protecting patient data in modern healthcare systems?

A) **Trust but verify** – Systems assume that internal users are trustworthy, but external access is heavily monitored.
B) **Least privilege principle** – All users and devices are granted the minimum level of access necessary to perform their tasks, and access is reviewed periodically.
C) **Perimeter-based security** – Securing the network by placing a strong barrier between internal systems and the external world, focusing on keeping threats out.
D) **Continuous verification and no inherent trust** – No user, device, or system is trusted by default, whether inside or outside the network. Every access request is verified before granting permissions.

Trivia:

Question:
Which of the following is the most comprehensive strategy for protecting yourself against advanced cybersecurity threats, such as phishing, ransomware, and data breaches?

A) Using strong, unique passwords and regularly changing them across all accounts
B) Implementing two-factor authentication (2FA) and using encrypted communication tools
C) Regularly updating software and installing security patches on all devices
D) A combination of strong password management, two-factor authentication, software updates, employee training, and network segmentation

Trivia:

Question:
Which of the following methods is **most likely** to allow ransomware or phishing attacks to infiltrate healthcare portals, despite cybersecurity measures in place?

A) Using outdated operating systems that are no longer supported with security patches
B) Employees falling victim to sophisticated spear-phishing emails that appear to be from trusted sources
C) Weak passwords on personal devices used to access healthcare portals remotely
D) Unencrypted data being transferred between healthcare systems

Future of Digital Healthcare

A. Interoperability and Unified Health Data Systems

- **Vision**: A more connected healthcare ecosystem where patient data seamlessly flows across platforms and providers, leading to more efficient and comprehensive care.
- **Key Drivers**: The push for interoperability through regulations such as the **21st Century Cures Act** and the development of frameworks like **TEFCA** (Trusted Exchange Framework and Common Agreement) aims to break down data silos.
- **Impact**: This will enable patients and providers to access a unified view of health records, improving decision-making, care coordination, and reducing duplication of tests or treatments.

B. Artificial Intelligence and Predictive Analytics

- **Vision**: AI-driven tools for diagnosis, treatment recommendations, and predictive analytics that anticipate patient outcomes and disease patterns.
- **Key Drivers**: Machine learning models are already being used for medical imaging, drug discovery, and patient risk stratification. As AI algorithms become more advanced and trustworthy, their role will expand.
- **Impact**: AI will enable more personalized medicine, improving outcomes by predicting complications, recommending preventive measures, and assisting in clinical decision-making.

Future of Digital Healthcare

C. Telehealth and Remote Patient Monitoring

- **Vision**: The pandemic accelerated the adoption of telemedicine, and this shift toward virtual care is expected to become permanent, especially for chronic disease management, follow-up visits, and mental health services.
- **Key Drivers**: Advances in wearable technology, remote patient monitoring (RPM), and connected devices allow continuous tracking of vital signs and real-time health updates.
- **Impact**: Patients will have greater access to care regardless of geography, and providers will be able to monitor and intervene early in case of health deterioration, potentially reducing hospital readmissions.

D. Patient Empowerment through Health Apps and Wearables

- **Vision**: Patients will take a more active role in managing their health through the use of apps and wearables that track everything from daily activity and nutrition to blood pressure and glucose levels.
- **Key Drivers**: Consumer-facing devices like smartwatches, fitness trackers, and mobile health apps continue to grow in sophistication, offering actionable health insights and fostering engagement.
- **Impact**: Empowering patients with real-time data will encourage preventive care and early intervention, reducing the overall burden on healthcare systems and improving health outcomes.

Future of Digital Healthcare

E. Data Security and Privacy Protections

- **Vision**: As digital healthcare grows, so too will the need for stronger protections against cybersecurity threats such as ransomware and data breaches.
- **Key Drivers**: Healthcare remains a prime target for cyberattacks, and stricter regulations (like GDPR in Europe) alongside technological advancements in encryption and blockchain may help protect sensitive data.
- **Impact**: Secure data exchange and storage will become a competitive advantage for healthcare providers, ensuring patient trust and compliance with regulatory standards while minimizing the risk of costly breaches.

F. Personalized Medicine and Genomics

- **Vision**: The integration of genetic data into healthcare will lead to highly personalized treatments, tailored to individual genetic profiles, thus enhancing the effectiveness of therapies.
- **Key Drivers**: Advances in genomics and biotechnology, as well as the decreasing cost of sequencing technologies, will make personalized medicine more accessible and mainstream.
- **Impact**: Precision medicine will improve patient outcomes, particularly in areas like oncology, where treatments can be tailored to the genetic mutations driving cancer growth.

Future of Digital Healthcare

G. Automation and Robotic Assistance

- **Vision**: Robotic process automation (RPA) and AI-driven tools will automate administrative tasks, streamlining workflows, and freeing up healthcare professionals to focus on patient care.
- **Key Drivers**: The need to reduce administrative burden, combined with advancements in AI and robotic technologies, will lead to more automation of tasks like appointment scheduling, billing, and even aspects of surgery.
- **Impact**: Automation will increase operational efficiency, reduce errors, and enhance the patient experience by making healthcare services more accessible and timelier.

Trivia:

Question:
Which technological advancement is **most likely** to drive personalized medicine and improve treatment outcomes in areas like oncology?

A) The widespread use of artificial intelligence in diagnostic imaging
B) The integration of genetic data into electronic health records (EHRs)
C) The growth of telemedicine and virtual health consultations
D) The automation of administrative processes through robotic systems

Trivia:

Question:
What is the **most critical factor** in ensuring widespread adoption of remote patient monitoring (RPM) in managing chronic conditions?

A) The development of user-friendly wearable devices
B) The regulatory push to mandate RPM for all healthcare providers
C) Improved cybersecurity measures to protect patient data
D) Patients' ability to understand and act on real-time health data

Trivia:

Question:
Which approach is **most likely** to build patient trust in digital healthcare systems while addressing concerns about privacy and security?

A) Mandating stronger passwords and multi-factor authentication for all users
B) Increasing the transparency of how healthcare data is used and shared
C) Transitioning entirely to blockchain technology for secure data transfer
D) Encrypting all patient data during storage and transmission

Today's Agenda

Thank You!

Community Health Survey: Your Input is Needed!

Scan the QR code to take survey or visit NuvanceHealth.org/community

- Only 10 minutes to complete!
- Individual responses are anonymous and confidential.
- 18 years old and over can complete.
- Share with your friends and family!
- Results will be used to develop health programs in your area.
- Languages available:
  - English
  - Spanish
  - Portuguese
  - Haitian Creole