Digital health

April 2022

U.S. Chamber of Commerce

Issue overview

Digital advancements are propelling innovation and driving long-term structural changes in how healthcare is delivered. Whether applied to the research ecosystem for new medicines, the electronic infrastructure of healthcare centers, or to care delivery for rural populations, digital health technology is central to our ability to innovate and deliver high-quality care.

The COVID-19 pandemic has exponentially accelerated the adoption of digital technology in health and underlines the importance of more robust global governance to ensure maximum benefits for patients and innovators. Future digital health tools will provide solutions to current unmet medical needs and, therefore, greater R&D investment in this space is imperative for the advancement of global health.

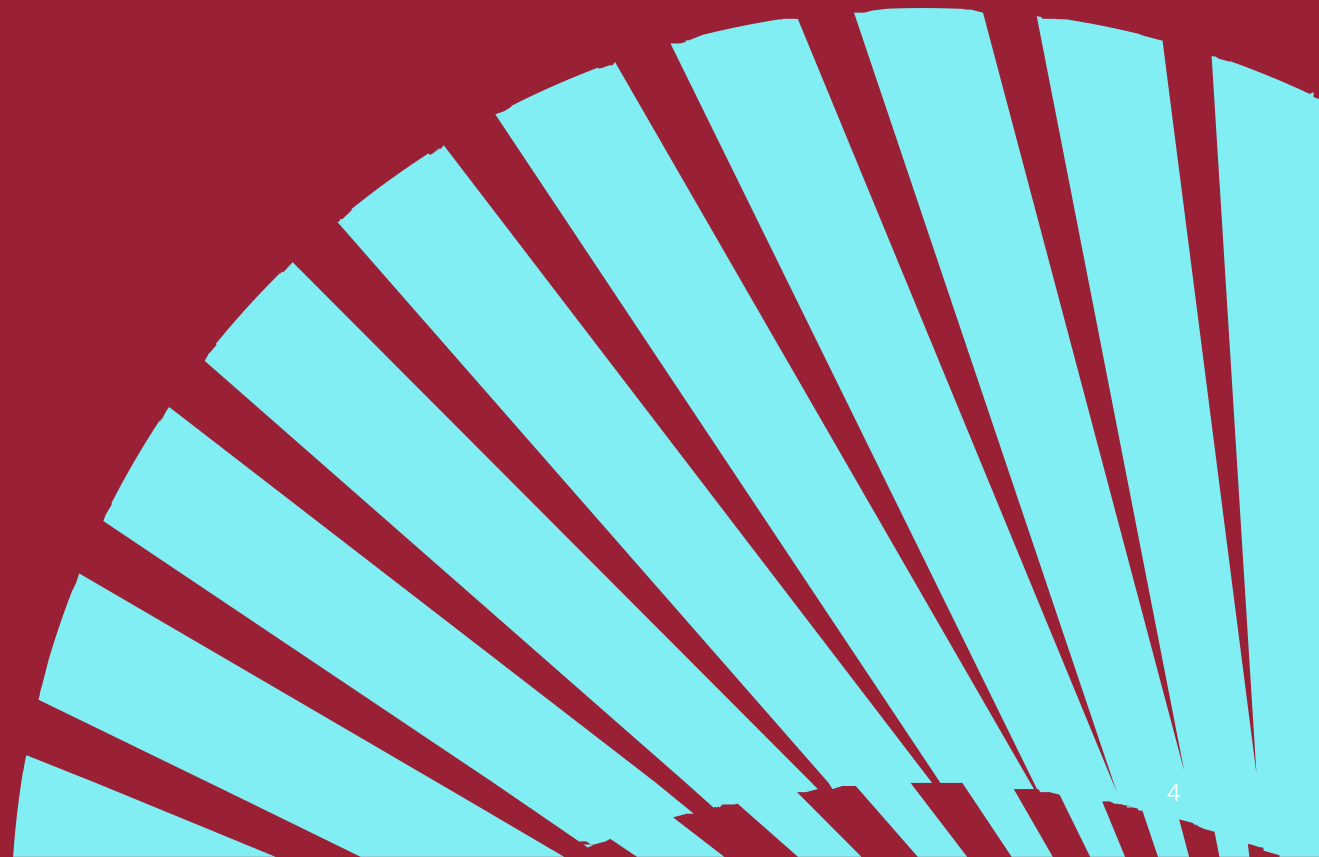
Providing access to, and affordability of, digital health tools to global communities will remain a challenge. The public and private sector must work together to bridge the digital gaps present in societies to ensure that disadvantaged populations can also benefit from these new digital health tools.

Positioning statement

We support policies and regulatory frameworks that embrace and promote digital technologies in healthcare to care for and monitor patients across all settings, enhance biomedical breakthroughs, and support public health surveillance. Although digital health has substantially increased during the COVID-19 pandemic, digital health should not only be leveraged during times of crises but also to address ongoing health systems strengthening efforts.

Policymakers have a critical opportunity to craft policies, regulations and standards that work to enhance government and private sector competitiveness strengthen and harmonize global standards around data flows, data interoperability, data privacy and protection, and improve investment to catalyze R&D around emerging technologies like AI and machine learning. The private sector, as the primary developer of digital health tools, is a critical partner to governments when crafting digital policies that are both feasible and promote growth.

Our core principles



Cross-border data flows are essential to advance public health and facilitate business in the global digital health economy

Protectionist measures by foreign governments, including data localization requirements and data transfer restrictions, inhibit patients from benefiting from new digital health tools.

Data should not be restricted to where it was originally generated, rather it should move to where it is needed to provide optimal health care.

By supporting open data flows, health systems are better served, and patient outcomes can be enhanced as clinicians, researchers, and patients themselves have access to more complete information to drive decision-making.[1]

Open and Protected Data Flows Foster Biomedical Advancements and Savings

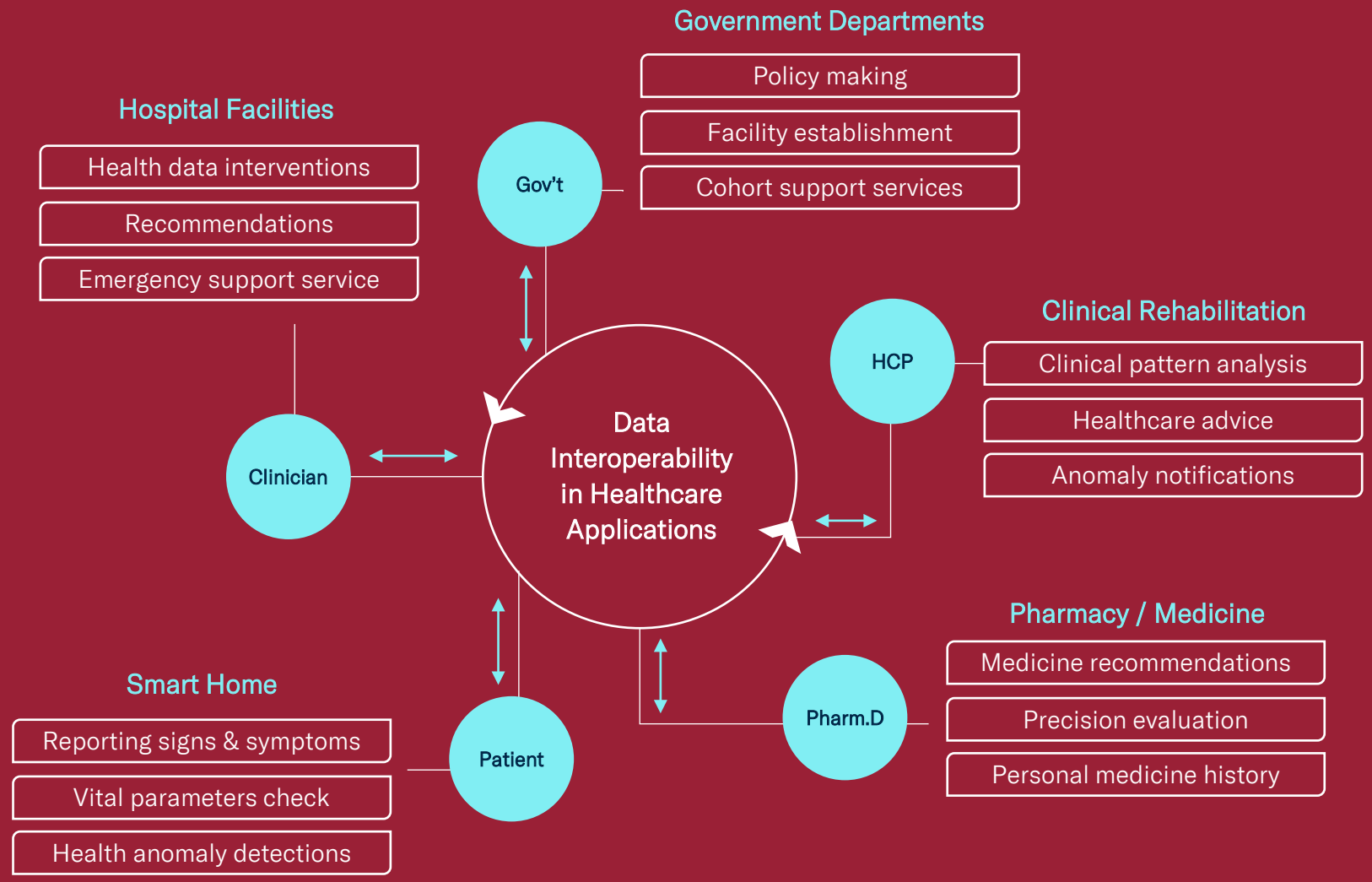
The cross-border sharing of genomic sequencing and bioinformatics data have allowed for one of the largest collaborations between public health and private sector biomedical innovators in surveilling and responding to the pandemic[1]

$1.1B of savings could be realized through cross-border data flows for each new drug developed[1]

Interoperability policies ensure that health IT infrastructures and devices can effectively interact, preserve data integrity and offer flexibility

As patients' care is increasingly distributed across multiple virtual and in-person care sites, data interoperability between platforms and devices can be established via technical specifications that are harmonized to a global standard to optimize patients' access to care.

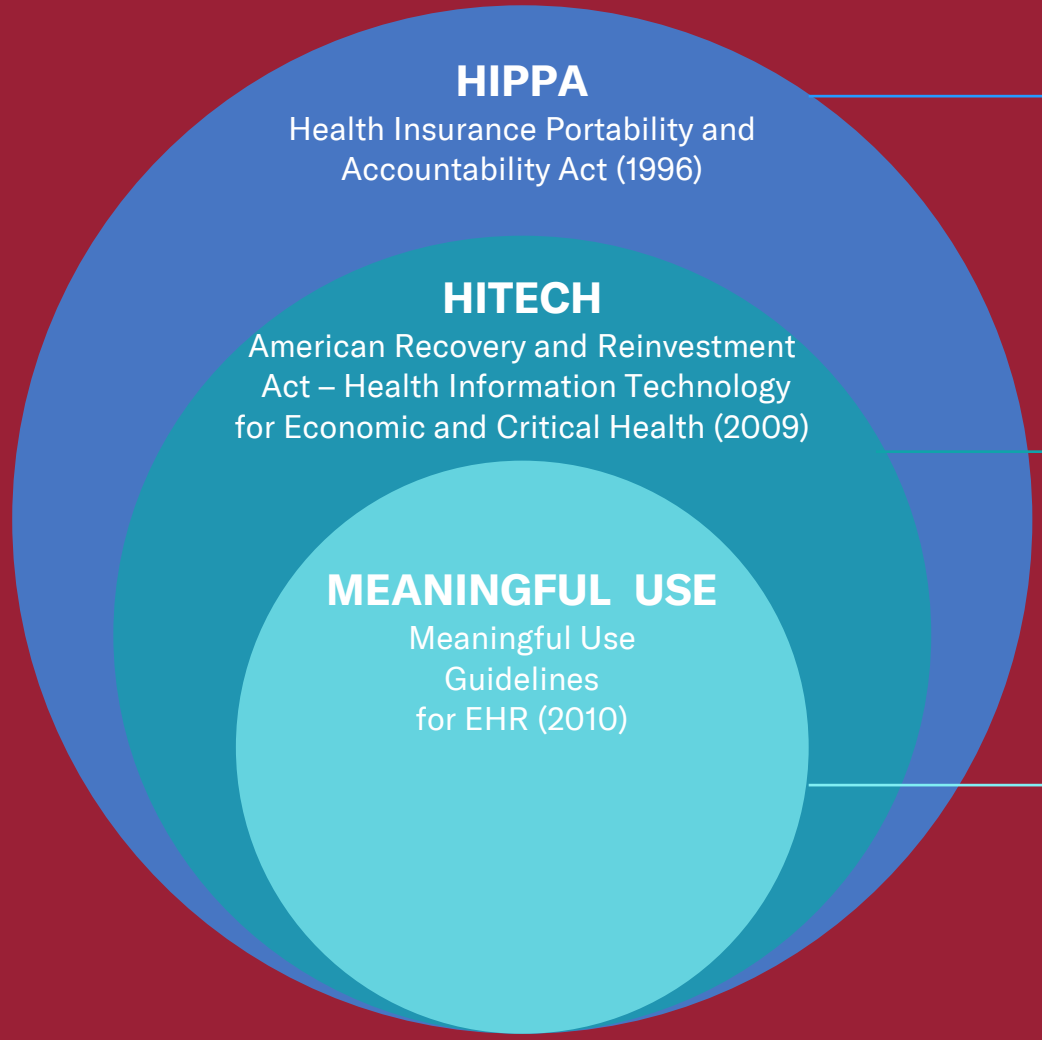
Despite progress, the lack of interoperability between clinical systems continues to impede patient care. In a recent study, only 15% of provider organizations felt patient data retrieved from another system benefited patient care to the extent that it should. [2]



Strong data privacy protections are essential to protect patients' data

As greater digital data is collected from patients, privacy should always be protected while health information remains accessible.

CASE STUDY: Establishing Policy Standards in the United States to Protect Patients' Confidential Information and Ensure That Health Data Remains Secure[3]



The goal of HIPPA was to protect patients' confidentiality amid increasing health data transfers aimed at enabling healthcare organizations to purse initiatives to further innovation

HITECH contained specific incentives designed to accelerate adoption of electronic health records system among providers – extending a new HIPPA Security Rule

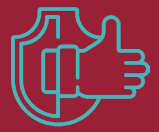
CMS' Meaningful Use measures created an incentive for eligible professionals and hospitals to use efficient electronic health records and encourage compliance measures to secure patient confidential information

Trust in AI and machine learning technologies is necessary to advance its responsible development, deployment and use

As digital health becomes increasingly reliant on AI technology, governments must partner with the private sector, academia and civil society to ensure patient confidence

Health executives trust AI to streamline administrative processes and provide more effective patient care with enhanced experiences for both patients and providers[4]

Patients report that their clinicians should act as a safeguard to buffer patients from the potential harms that might result from mistakes made by healthcare AI[4]

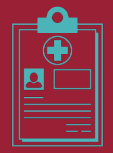


Patients want to ensure that AI healthcare decisions are not be based on flawed datasets[4]

From wearables and health apps to virtual healthcare services, U.S. consumers report that these advanced technology is important to healthcare management[5]

Application of AI and Machine Learning in Healthcare[6]

Algorithms and statistical models assist doctors by processing and analyzing large data sets



Patient medical history

Savings

Predictive Treatment Outcomes

Fostering public trust in AI is necessary to advance its responsible development, deployment and use[7]

Governments should work together and commit to flexible, risk-based frameworks that encourage AI innovation and collaborate across borders to advance sound and interoperable practices

When appropriately regulated, AI has the potential to act as a force for good, tackling challenges and spurring economic growth for the benefit of consumers, businesses, and society.

Investments in cybersecurity are essential to protect patients' data, ensure uninterrupted care, and secure the entire health ecosystem

Healthcare companies, networks and providers are not immune from cyberattacks and data intrusions, requiring the sector to ensure baseline cybersecurity safety measures.

The integration of advanced digital technologies in health systems and related services has transformed the industry, resulting in measurable improvements in how healthcare is delivered. However, this integration also fosters a new set of challenges for patients, healthcare providers and manufacturers of healthcare goods and services.

It is critical that cybersecurity a strategic priority to both ensure patient safety and minimize enterprise risk.

The Implications of Cybersecurity in Healthcare

15%

Predicted year-over-year growth of the global healthcare cybersecurity market through 2025[8]

123%

Rise in the number of ransomware attempts against the healthcare industry, 2020-2021[9]

$20.8 b

Annual cost of ransomware attacks to healthcare companies in the U.S. due to downtime in 2020[10]

Impact of Cyber Attacks in Healthcare Can be Threefold[11]

Losses of Confidentiality
Exposure of personal data, triggers ripple effects including theft or loss of patient information

Losses of Integrity
Patients and practitioners lose confidence in a provider's ability to access the correct data

Losses of Availability
Data intrusions on operations systems can close facilities, disrupt care and damage infrastructure

References

1. Kepes, Rozi., White, Joshau., Yeater, Aaron. The Importance of cross-border data flows (2021). https://about.fb.com/wp-content/uploads/2021/06/The-Importance-of-Cross-Border-Data-Flows.pdf
2. College of Healthcare Information Management Executives (CHIME), KLAS Research. Trends in EMR Interoperability (2021). https://chimecentral.org/wp-content/uploads/2021/01/Trends-in-EMR-Interoperability_CHIME_KLAS.pdf
3. SecureWorks. Blog Post: The Human Side of Healthcare Data Security (2012). https://www.secureworks.com/blog/general-the-human-side-of-healthcare-data-security
4. Optum. AI Survey: Health Care Organizations Continue to Adopt Artificial Intelligence to Help Achieve Better, More Equitable and Affordable Patient Outcomes (2021). https://www.optum.com/about-us/news/artificial-intelligence-equitable-affordable.html
5. Richardson, Jordan P., Smith, Cambray. et al. Nature. Patient apprehensions about the use of artificial intelligence in healthcare (2021). https://www.nature.com/articles/s41746-021-00509-1
6. SevenTablet. Blog post. How Machine Learning and AI Benefit Healthcare [Infographic] (2021). https://7t.co/blog/how-machine-learning-and-ai-benefit-healthcare-infographic/
7. US Chamber of Commerce. Special Report. The Digital Trade Revolution: How U.S. Workers and Companies Can Benefit from a Digital Trade Agreement (2022). https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022_2022-02-09-202447_wovt.pdf
8. Morgan, S. Cybercrime Magazine. Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 To 2025 (2020). https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/
9. SonicWalll. Annual Report. 2022 SonicWall Cyber Threat Report (2022). https://www.sonicwall.com/2022-cyber-threat-report/
10. Bischoff, P., comparitech Blog Post. Ransomware attacks on US healthcare organizations cost $20.8bn in 2020 (2020). https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
11. Snair, J., Henry, D. NACCHO. Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable (2013). https://www.naccho.org/blog/articles/risks-of-cyber-attacks-on-the-healthcare-sector-leave-public-health-of-communities-vulnerable