Public Health Tech Initiative:

Using Health Technology to Respond to Public Health Emergencies

November 2021

Consumer Technology Association™

Introduction

The COVID-19 pandemic was an unprecedented event for which no nation, including the U.S., could have been fully prepared.[1] The world initially grappled with understanding the depth and breadth of the threats that the virus posed to diverse populations. While the U.S. quickly responded to the pandemic using previously tested methods based on pre-planning, some challenges and unexpected circumstances emerged from the novel virus. Coordination of resources across federal and state governments and effective partnerships with the private sector proved vital in the pandemic response. There were several "lessons learned" during the pandemic that are worth considering in preparation for future events. For example, clinicians can provide health care services effectively without consumers having to go to a health care facility, and remote clinicians and caregivers working together can monitor patients to manage chronic conditions. Most importantly, we learned that clinicians and consumers can quickly adapt to providing and receiving services virtually.

However, despite extensive disaster preparedness planning, the pandemic shined a light on several weaknesses in our health care system including underfunded state and local public health agencies, fragmented health data, fragile supply chains, inequitable care and outdated health-related laws and regulations.

This paper sets out a framework for leveraging these "lessons learned" from the pandemic for improved planning, response, coordination and remediation moving forward with public and private partnerships that leverage resources for effective results.

Background

The Consumer Technology Association (CTA)® believes that the increasing reliance of health technology during the pandemic is a unique opportunity to advance the greater use and adoption of trustworthy digital health to improve the country's response in future public health emergencies.

With that in mind, we created the Public Health Tech Initiative ("PHTI" or "the Coalition" or "we"), a group of almost 20 organizations consisting of leading health systems, technology companies, medical device manufacturers, health insurance providers, public policy organizations and medical societies.

The coalition's work has been divided into two areas of focus:

- Digital health, the technology-based health care solutions particularly suited to address public health emergencies and identify the barriers that prevent greater use of these solutions.
- Data and privacy, specifically the impact health data has on managing public health emergencies, privacy concerns and the impact the lack of data sharing may have on effective use of health technology in public health emergencies.

This paper discusses the fragmented nature of our public health system, the role digital health and data use have played in response to COVID-19, and the legal and operational barriers that prevented the more effective use of digital health and health data during the pandemic. We have also developed a series of recommendations highlighting ways in which health technology may be more successfully used in addressing public health emergencies.

The report examines how greater and appropriate use of digital health technology can play a more significant role in planning for, and responding to, future public health emergencies. While the report is the work of the Coalition, its recommendations are consistent with overarching CTA principles.

MEMBERS OF PHTI:

AHIP, American College of Cardiology, Brookings, Doctor on Demand, Health Innovation Alliance, Humana, Humetrix, Kinsa Health, Microsoft, Northwell Health, Philips, ResMed, Roche Diabetes Care, SSM Health, UCHealth, Xealth. The Coalition is co-chaired by Dr. David Rhew, Chief Medical Officer at Microsoft, and Dr. Alex Garza, the Chief Community Health Officer at SSM Health.

About

Consumer Technology Association™

As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the most influential tech event in the world.

COVID-19 Overview

The history of COVID-19 is familiar to most. In late December 2019, Chinese health authorities reported a cluster of people who had contracted a pneumonia-like disease in Hubei Province.[2] By mid-January 2020, China officially recorded its first death linked to the novel coronavirus quickly followed by the first reported coronavirus infection outside of China—in Thailand.

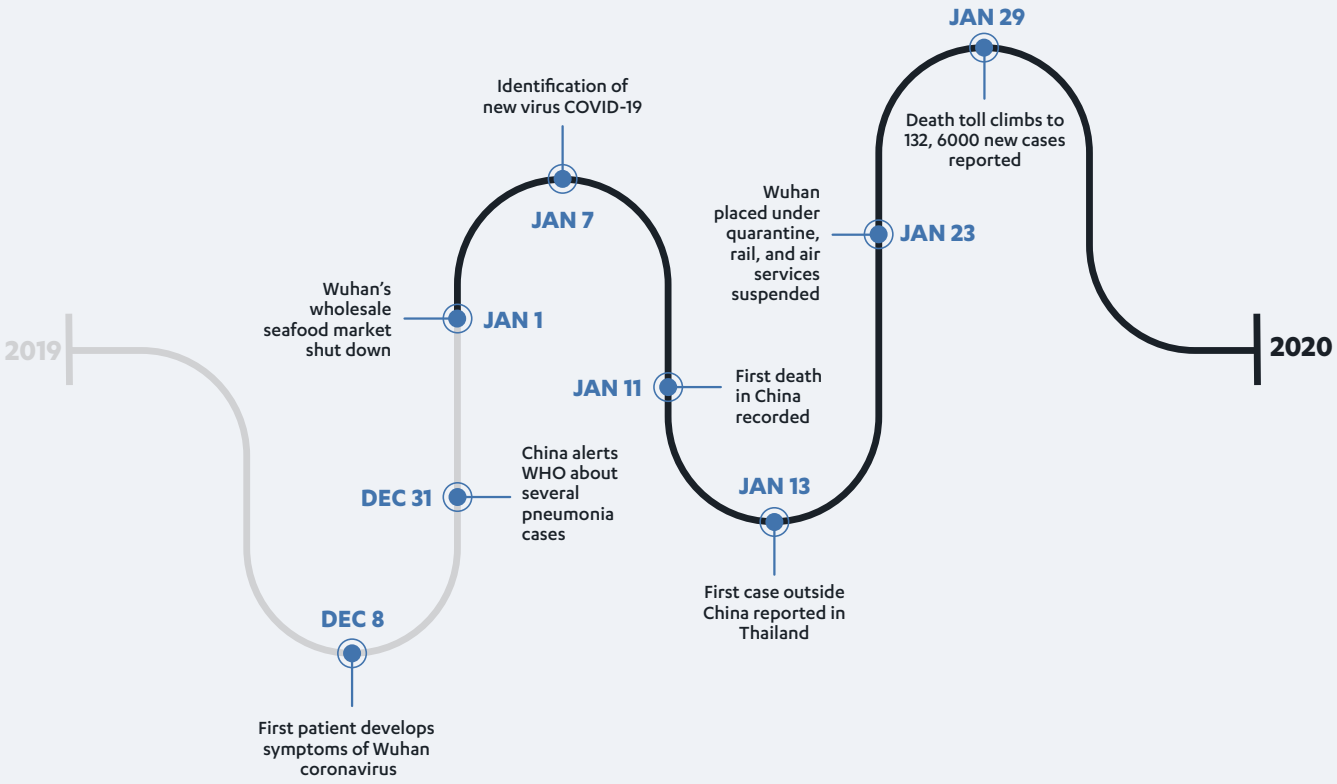
By late January 2020, the World Health Organization ("WHO") declared the new coronavirus a Public Health Emergency of International Concern—only the sixth time that such an emergency had been declared by the WHO. At the time there were almost 8000 officially confirmed cases in China with about 170 deaths from those cases. Outside of China, there were about 100 reported cases and no deaths in 18 countries.[3]

Meanwhile in the U.S., on January 19, 2020, a 35-year-old man went to an urgent care clinic in Snohomish County, Washington, after returning from Wuhan visiting family—and became the first official COVID-19 case in the U.S.[4] The first U.S. fatality from the coronavirus came the next month.[5]

As the virus started to spread, in March 2020, President Trump issued an emergency proclamation giving the Department of Health and Human Services ("HHS") the authority to temporarily waive or modify certain requirements of the Medicare, Medicaid andstate Children's Health Insurance Programs and the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule.[6] By the end of March, the U.S. experienced a significant surge in COVID-19 cases and deaths.[7]

Despite these challenges one of the bright spots in the nation's response to the pandemic has been the increased adoption of digital health technology.

FIG. 1 CORONAVIRUS TIMELINE: THE BEGINNING



Source: weforum.org

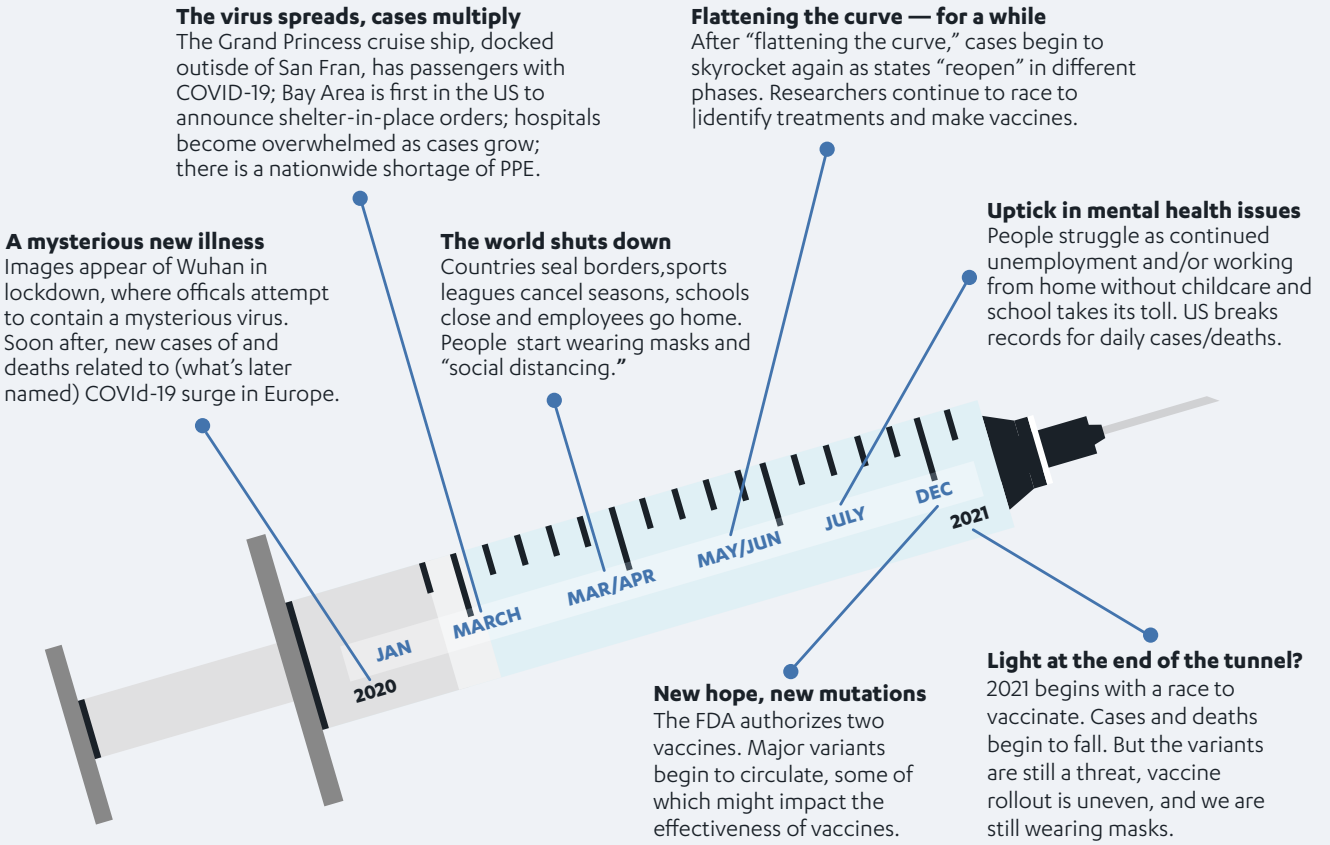
Public Health

To understand the United States' response to the pandemic, it is important to first understand the basics of public health and how the American public health system works. Public health is the science and art of preventing disease and promoting health through the organized efforts and informed choices of society, organizations, public and private communities and individuals.[8]

Most public health experts believe that public health agencies should have the following functions:

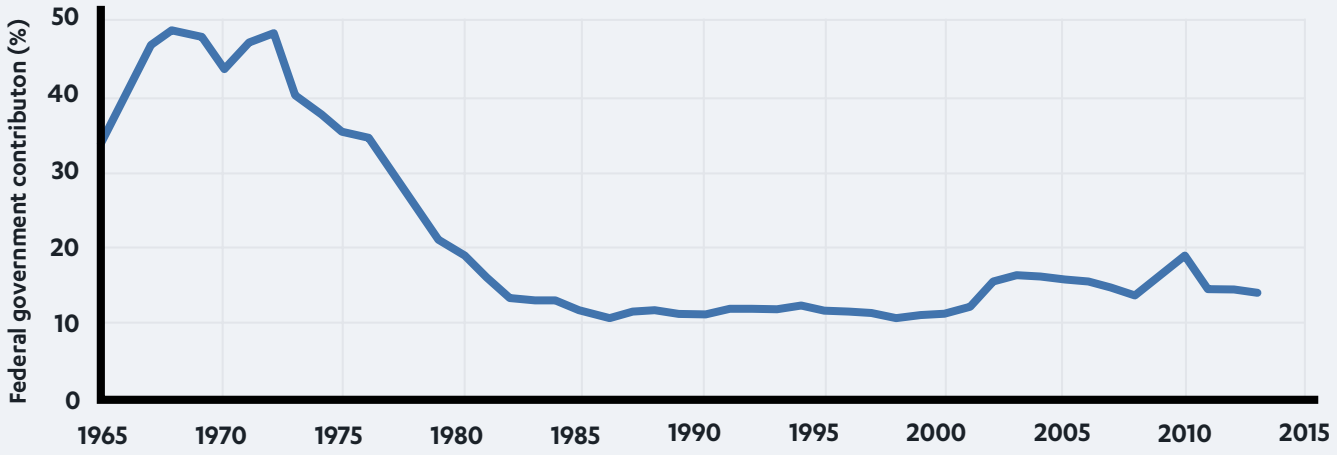
- Investigate, diagnose and address health problems and hazards affecting the population.
- Communicate effectively to inform and educate people about health, factors that influence it and how to improve it.
- Strengthen, support and mobilize communities and partnerships to improve health.
- Create, champion and implement policies, plans and laws that impact health.
- Utilize legal and regulatory actions designed to improve and protect the public's health.
- Assure an effective system that enables equitable access to the individual services and care needed to be healthy.
- Build and support a diverse and skilled public health workforce.
- Improve and innovate public health functions through ongoing evaluation, research, and continuous quality improvement.
- Build and maintain a strong organizational infrastructure for public health.[9]

FIG. 2 COVID-19 TIMELINE



Source: ysm-res.cloudinary.com

FIG. 3 FEDERAL GOVERNMENT SHARE OF TOTAL PUBLIC HEALTH EXPENDITURES



Source: milbank.org

The U.S. public health system is made up of a complex network of people and organizations in the public and private sectors who work with varying degrees of collaboration at national, state and local levels.[10] The system includes a wide array of governmental and non-governmental entities such as:

- About 3000 county and city health departments and local boards of health.
- 59 state and territorial health departments
- Tribal health departments.
- More than 160,000 public and private laboratories.
- Parts of multiple federal departments and agencies.
- Hospitals and other health care providers.
- Health insurance providers
- Volunteer organizations.[11]

The organization of public health at the federal level is driven by HHS and its agencies such as the Centers for Disease Control and Prevention ("CDC") (the nation's lead public health agency), the Food and Drug Administration ("FDA"), the National Institutes of Health ("NIH") and the Centers for Medicare and Medicaid Services ("CMS").

Public health responsibilities at both the state and local levels are divided among multiple agencies, in addition to the principal public health agency—with each state having its own framework for public health.[12] The pandemic amplified the difficulty associated with coordinating across these varied entities within a complex structure.

While there were significant increases in public health funding after the terror attacks of 9/11, mainly for biosurveillance and biosecurity, subsequent funding decreases caused significant staffing cuts of about 50,000 staff positions at local public health departments nationally. A smaller proportion of public health spending is now coming from the federal government with estimates showing federal government public health spending under $100 billion annually before the pandemic—or 2.5% of total federal government health care spending.

Studies looking at actual spending on a population-wide level, however, estimate spending to be more likely between $35 billion and $65 billion annually—or 1.5% of total health spending. In other words, official estimates are likely tens of billions of dollars higher than actual spending.[13]

The American Rescue Plan Act of 2021, signed into law by President Biden in March 2021, provides increases in spending for initiatives such as hiring

and training more public health workers for federal, state and local governments, the creation of a new public health corps and recruiting and training future public health leaders.[14] The renewed emphasis on bolstering public health is important, but longstanding underinvestment in public health cannot be overturned with increased short-term funding. To be better prepared for future public health emergencies, the U.S. needs to build and sustain a coordinated and robust public health system.

Digital Health and the Pandemic

Digital Health During COVID-19

Digital health is the use of technology and electronic communications tools, services and processes to deliver health care services or to facilitate better health. It includes a diverse array of technology and services including telehealth, remote monitoring, AI-enabled solutions, apps, trackers and digital therapeutics.[15] During the COVID-19 pandemic, the use of digital health surged but it remains unclear whether it will become a permanent feature of the health care system. In addition, health insurance providers and other stakeholders will need to meet the increased consumer demand for digital health.

As captured in a CTA research paper published earlier this year, the surge in the use of digital health (particularly of telehealth) was dramatic.[16]

- Remote care solutions became many providers' sole method for reaching their patients and many consumers' only way to access non-emergency health care services safely.
- As of May 2020, consumer-reported adoption of remote health consultation services nearly tripled year-over-year. 41% of U.S. broadband households reported that at least one household member used a service to remotely consult with a doctor or other health care provider in the previous 12 months, up from just 15% in Q2 2019.
- An internal CMS analysis of Medicare fee-for-service claims data from March 17 to June 13, 2020, revealed that more than 9 million Medicare beneficiaries received telehealth services—a significant increase from the approximately 52,000 per month that received such services per month prior to COVID-19.
- 32% of households with an annual income of less than $30,000 used a telehealth service in the previous 12 months, compared to 12% in Q2 2019.
- 24% of those who self-identify as technology laggards (i.e., buying new technology only once traditional alternatives are no longer available) used a telehealth service, up from 6% in Q2 2019.

As of May 2020, 42% of consumers report owning at least one internet-connected health device that has the capability to track their health metrics over time.[17] A report from the Kaiser Family Foundation analyzing the Medicare program has similar findings.[18]

- More than 1 in 4 Medicare beneficiaries had a telehealth visit between the summer and fall of 2020.
- Among the majority of Medicare beneficiaries with a usual source of care (95%), such as a doctor or other health professional, or a clinic, nearly two-thirds (64% or 33.6 million) say that their provider currently offers telehealth appointments—up from 18% who said their provider offered telehealth before the pandemic.
- Prior to COVID-19, telehealth utilization among Medicare beneficiaries was extremely low—with only 0.3% of traditional Medicare beneficiaries enrolled in Part B using telehealth services in 2016, accounting for only 0.4% of traditional Medicare Part B spending.

DOCTOR ON DEMAND®

Founded in 2012, Doctor On Demand® provides virtual care via on-demand and scheduled visits with its team of dedicated health care providers across the U.S. The company provides solutions for employers and health plans, as well as offers direct-to-consumer services. During COVID-19, Doctor On Demand® saw skyrocketing patient and caregiver demand across its medical and mental health services, with utilization in March and April 2020 roughly three times that of normal volumes.

In February 2020, at the onset of the COVID-19 outbreak, the company launched a coronavirus resource center and coronavirus risk assessment to help patients prepare for the impending global pandemic. The company continuously updated their assessment tool to meet evolving guidelines and to effectively serve as a triage tool for patients seeking care. In May 2020, the company expanded its medical services to include Medicare Part B coverage following the Centers for Medicare & Medicaid Services' expansion of telehealth services in response to the COVID-19 outbreak. To support its senior patients, Doctor On Demand® waived copays for its Medicare Part B customers during the COVID-19 health crisis. The company also launched the ability for patients to book same-day mental health visits with psychologists and psychiatrists to close access disparities and meet the increasing demand for mental health care from home.

In 2020, Doctor On Demand® reached nearly 98 million covered lives, while continuing to grow their Virtual Primary Care offering, integrated behavioral health, 24/7 everyday & urgent care and chronic care management.

MICROSOFT®

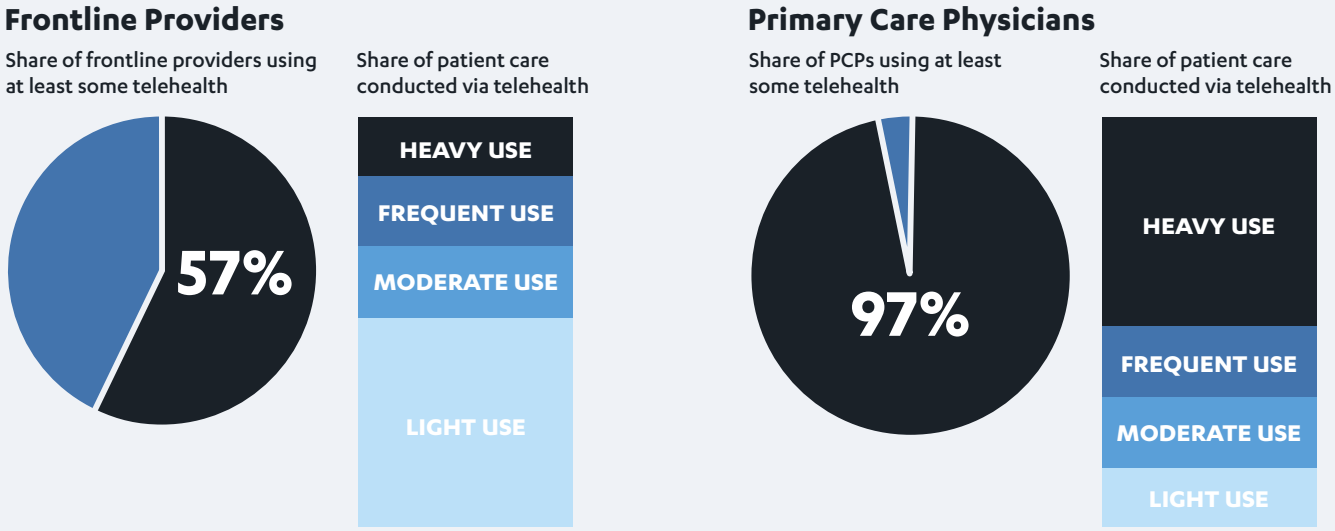
Microsoft® is a global enterprise company whose cloud-based technologies provide the underlying data platform for health care organizations and government agencies across the globe. As a result, Microsoft® was engaged early during the pandemic to provide technology assistance for those battling COVID-19 and provided technology and services through its Microsoft Services Disaster Response ("MSDR") program. MSDR completed 71 projects in 2020 and continues to provide services. The projects are COVID-19 relief efforts requested by governments and not-for-profit organizations around the world. Among other things, the company developed and deployed COVID-19 screening and triage bots, mobile apps for field workers, dashboards and analytics for public health agencies and migrations to Azure to enable population health data management. Microsoft® and its partners also developed vaccine management solutions including facilitating registration functionality for patients and clinicians, phased scheduling for vaccinations, streamlined reporting and management dashboarding with analytics and forecasting. Microsoft® is also working with the World Health Organization to create the world's first comprehensive, end-to-end data solution for global health (the World Health Data Hub).

NORTHWELL HEALTH®

Northwell Health® is the state of New York's largest health care provider and private employer, with 23 hospitals, 830 outpatient facilities, more than 16,600 affiliated physicians and almost 19,000 nurses. Between March 16 and April 7, 2020, COVID-19 hospitalizations within Northwell Health® increased from 49 to 3425, overrunning the system's emergency departments and urgent care centers. In response, the system added nearly 2000 beds, filling up space in lobbies, auditoriums, operating rooms, catheterization labs and other rooms that were standing empty after Northwell canceled electives on March 16, 2020. Northwell Health® additionally took responsibility for a 1000-bed field hospital staffed by Army clinicians and a 1000-bed Navy hospital ship docked in Manhattan. Adding additional beds only solved part of the capacity issue. The other major component was staffing, particularly staffing of providers with critical care training. In response, Northwell Health® made permanent infrastructure changes by increasing its use of telemedicine carts from Amwell®.

During the height of the COVID-19 pandemic, these carts allowed the system to staff its increased number of ICU beds beyond the traditional Tele ICU. Nurses and providers without critical care training were able to care for patients under the guidance of those with such training by doing so. To continue providing care for patients with non-COVID-19 medical problems, Northwell Health® exponentially expanded its telehealth offerings, expanding access from 200 practitioners to 6200. While prior to the COVID-19 outbreak, Northwell Health® saw 100 to 200 telehealth visits per year, during the height of the COVID-19 crisis in New York, it saw 5000 to 8000 per day. From March 1 to April 30, the system conducted 112,000 telehealth visits throughout its entire health system. Today Northwell Health® averages between 1000 and 1200 visits (both audio/video and audio only) per weekday as office visits have returned to pre-pandemic levels.

FIG. 4 TELEHEALTH BECOMES THE FIRST LINE OF TREATMENT FOR A MAJORITY OF U.S. PATIENT CARE AMID COVID-19



Source: bain.com

But telehealth is not the only way in which digital health and health technology have been effectively used during the pandemic.[19] Remote patient monitoring allows health care providers to monitor people who have contracted COVID-19 and are isolating at home as well as non-COVID-19 patients who health care providers did not want appearing in overstressed hospitals and physician offices.[20]

Chatbots, which use artificial intelligence ("AI") tools to facilitate communications between users and software applications, have been an important component of responding to the virus. The WHO developed a chatbot which has reached millions of people looking for information about the coronavirus or monitoring symptoms.[21] Many health care stakeholders built similar chatbots to great effect.[22]

Additionally, wearable technology has been used by consumers to measure certain physiological functions like blood oxygen levels, heart and respiration rates, sleep duration and body temperature—all which can be important factors in monitoring potential COVID-19 symptoms.[23]

WHAT IS "TELEHEALTH"?

What is "telehealth"? The answer depends on who is answering the question. More confusing still, the terms "telehealth" and "telemedicine" are increasingly used interchangeably. Historically, "telehealth" referred to a broad scope of remote health care services (including non-clinical services such as training and education) while "telemedicine" described actual clinical practice—via telecommunications technology. For purposes of this paper, and reflecting industry standards, we will be using the terms "telehealth" and "telemedicine" interchangeably, unless one of the terms is specifically used in a particular context—such as laws and regulations. For purposes of this paper, "telehealth" means the delivery of health-related care, services, education, and information via telecommunication technology—not to be confused with the with the CMS or other payers' definitions of telehealth "telehealth."

KINSA HEALTH®

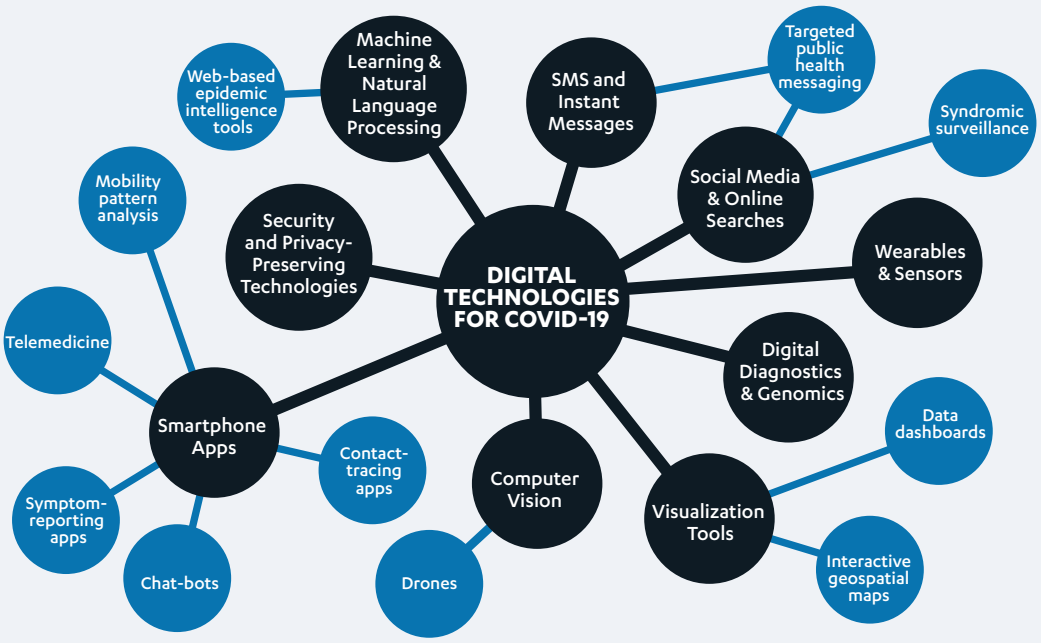
Over the past nine years, Kinsa® has built a next-generation early warning system, based on syndromic surveillance principles, to support households, communities and public health systems with earlier and more actionable information about when and where infectious illness will spread. The company's network enables accurate local forecasts of influenza-like illness months in advance and provided up to a three-week early indication of COVID-19 hospitalization and deaths. Today, more than 2 million households, 5% of U.S. elementary schools and numerous companies are part of a network that use Kinsa® illness triage applications, smart thermometers and illness response systems. Through their use, Kinsa® aggregates unique illness insights not available elsewhere: real-time intra-household, intra-school and intra-grade transmission patterns; symptom incidence and prevalence from mildly symptomatic people; and symptom progression throughout the course of illness. This is information the health care system largely misses, yet Kinsa® captures to accurately detect, monitor and forecast both emerging biothreats and existing ones like cold and flu. Additionally, the company has the unique ability to survey sentinel households and schools that may be exposed to illness more frequently and earlier on during an outbreak due to the contact networks of their populations. Through a real- time two-way communication system, Kinsa® ascertains more information about illness exposures and delivers guidance and education to the user. This enables additional insights in the context of an outbreak.

UCHEALTH®

UCHealth® is a large, integrated network of hospitals, clinics and practices, headquartered in Colorado, made up of more than 24,000 employees providing community-focused medicine. Partnering with industry, UCHealth® developed interactive and dynamic clinical decision support tools fully integrated within the electronic health record and provider workflows allowing the health system to deploy new information and treatment recommendations for COVID-19 across 12 hospitals and thousands of providers rapidly and seamlessly. As diagnostic and treatment modalities changed, often hourly, these tools changed too—making up-to-the-minute management, testing and treatment information immediately accessible.

Well before UCHealth® began to see its numbers of hospitalized COVID-19 patients increase at the start of the pandemic, the health care system recognized that remote patient monitoring ("RPM") and other technology would be integral to caring for patients. COVID-19 patients were selected to participate in a pilot to test an FDA- approved RPM wearable that fits on their wrist and finger. An app downloaded to a smartphone transmitted the patient's biometric data so providers at UCHealth's® Virtual Health Center could monitor patients in real-time and react to problems such as decreased oxygen levels or increased respiratory and heart rates. This program allowed dozens of patients to avoid hospitalization, and for those who did require hospitalization, they were able to be discharged sooner—having an average length of stay of one day shorter. UCHealth® has cared for almost 10,000 patients with COVID-19 infections. More than 9000 have recovered and been able to return to their homes or to a post-acute care facility—many with the RPM device transmitting their biometric data to the Virtual Health Center.

FIG. 5 THE INTERCONNECTED DIGITAL TECHNOLOGIES USED IN THE PUBLIC-HEALTH RESPONSE TO COVID-19



Source: Nature.com

Data dashboards, a dynamic way to present real-time or near-real-time critical information, have been used by government authorities to manage outbreaks and assess response activities.[24] Dashboards were developed by governments, international organizations (like WHO),[25] academic institutions (like Johns Hopkins University),[26] and private industry. Drones and robotics have been used to deliver medical supplies, disinfect suspected infected areas and collect samples from remote areas.[27] And while AI has been incorporated in many of the digital health technologies discussed, it has also been used to predict and track the prevalence of COVID-19, as well as to help diagnose and treat the disease.[28] While some studies conducted early in the pandemic seemed to indicate that AI had not been impactful in fighting COVID-19, more recent studies show otherwise.[29]

Legal, Operational, Technological and Policy Changes During the Pandemic

Both federal and state governments increased coverage for digital health services (particularly telehealth) by expanding the scope of services that qualify for reimbursement under government health programs (like Medicare and Medicaid). Many health insurance providers also followed suit by voluntarily covering a broader scope of telehealth and digital health services. These measures, in addition to consumer demand, incentivized health care providers to adopt digital health (telehealth, in particular) in growing numbers as discussed above.

At the onset of the pandemic, CMS and Congress took unprecedented measures to drive the use of digital health, through existing and new authorities, effective for "the duration of the COVID-19 public health emergency," including the following:

- CMS waived limitations on the types of practitioners able to offer telehealth services to Medicare patients and added physical therapists, occupational therapists and speech language pathologists to the list of professionals eligible to bill Medicare for telehealth.[30] Congress suspended requirements regarding originating sites (i.e., the location from which a telehealth patient can receive care). Medicare beneficiaries can now receive telehealth services inside their own homes

rather than in a location (e.g., hospital, clinic, physician office) that meets the originating site requirements.[31]

- CMS added 135 additional allowable services to its list of services that can be delivered via telehealth, which more than doubled its service list.[32]
- CMS also allowed reimbursement for certain telephone evaluation and management visits for new patients as well as established patients—in addition to certain behavioral health services.[33]
- CMS adjusted payments to practitioners for certain telephone evaluation and management services to match payments for in-person visits.[34]
- CMS temporarily waived requirements that a billing provider be licensed in the state in which the provider renders services to a patient. Instead, the provider must be enrolled in Medicare, have a valid license in the state which relates to Medicare enrollment, furnish services in the state where the emergency is occurring, and not be excluded from practicing in that state or any other state that is part of the emergency.[35]

Later in the pandemic, CMS also announced the Acute Hospital Care at Home program, providing eligible hospitals the ability to treat eligible patients in their homes. Participating hospitals are required to have appropriate screening protocols before care at home begins.[36]

Other federal government agencies implemented additional waivers and policy flexibilities. For example:

- The HHS Office for Civil Rights ("OCR") announced that it would exercise enforcement discretion allowing the good faith use of popular video-chat applications by health care providers for telehealth, including FaceTime®, Zoom® and Skype®.[37] Health insurance plans were not covered by the OCR's enforcement discretion and AHIP, the industry's trade association and specific member plans have advocated that they should have been included to enable a better COVID-19 response.
- HHS, with the concurrence of the Drug Enforcement Agency issued a waiver regarding the Ryan Haight Online Pharmacy Consumer Protection Act of 2008—allowing prescription via a telehealth of a schedule II–IV controlled substances to a patient without the need for an in-person medical evaluation.[38]
- 47 U.S. states and three U.S. territories waived requirements regarding in-state licensure, originating sites, pre-existing relationships with physicians, the prescription of controlled substances and the use of audio-only telephone services.[39] Certain states also issued executive orders requiring health insurance providers to expand telemedicine coverage for all services that would normally be covered for an in-person visit. Some states also mandated payment parity for virtual and in-person visits.

The number and breadth of the waivers clearly show how many barriers to fuller adoption of digital health exist.

Barriers Preventing the Full Use of Digital Health to Support a Timely Pandemic Response

Despite all the waivers, federal and state laws and regulations failed to recognize the full spectrum of digital health services outside of telehealth. Strict laws and regulations generally limit the use of new or emerging health technology—telehealth and remote patient monitoring excepted—resulting in difficulty scaling digital health solutions that are not officially recognized or covered and reimbursed. This is particularly true with making changes to public programs like Medicare and Medicaid which often requires an act of Congress. The long and slow adoption of telemedicine in the U.S. provides a cautionary note for adopting other digital health categories in a swifter fashion. For example, states have implemented varying requirements related to practice standards (e.g., establishing a clinician/patient relationship), but most relate to telehealth. As technology-enabled care becomes more sophisticated, it is challenging

some of the basic notions of practice standards that are not reflected in current law or regulation.

Health care workforce training is also imperative. Technology implementation can be time-intensive and expensive and health care providers may not be sufficiently able to assess, adopt and implement new health information technology. Professional medical schools and training programs should be preparing providers to effectively use telehealth and emerging health information technology. Certain organizations are developing training criteria and programs for digital health, but many more are needed.[40]

Finally, without quality and affordable internet access, people are unable to fully access digital health services (including telehealth), effectively use many remote monitoring tools, access electronic medical records, or even research health conditions and treatment. Many consider access to broadband a social determinant of health.[41] A recent analysis found that almost 163 million people in the United States do not use the internet at broadband speeds.[42] Without appropriate connectivity, it is likely that adoption of digital health will stall, especially within unserved or underserved populations. The impact on the health of various communities due to the lack of access to broadband is analyzed in a separate paper by CTA® and the Connected Health Initiative on health equity issues.

Recommendations for Digital Health

Federal and state governments must develop a coherent and meaningful expansion of broadband coverage to ensure it reaches rural and underserved areas.

- Many digital health products and applications offered today work most effectively with a broadband connection. The range of the tools and the speed at which they are being made available to health care providers and consumers show it is critical that broadband service be accessible to all populations. While important steps have been taken toward this goal (for example, the $7 billion Emergency Connectivity Fund under the American Rescue Plan), much work needs to be done. We also note that even for many with access to broadband service, affordability and quality is an issue.

  Therefore, we urge Congress and the Federal Communications Commission ("FCC") to consider awareness and outreach support to connect consumers to broadband-based initiatives. Additionally, we recommend Congress encourage agencies such as CMS and the FCC to seek opportunities to expand access to technologies that facilitate access to video and audio care for unserved and underserved populations.

We urge Congress to make some of the Medicare telehealth COVID-19 public health emergency waivers and flexibilities permanent.

- Current Medicare laws and regulations unnecessarily limit coverage of telehealth to rural areas and require patients to be present at certain approved originating sites such as hospitals and physician offices to receive telehealth services. Waivers of the restrictions regarding geographic location and originating site should be made permanent. This will allow Medicare fee-for-service beneficiaries to continue to receive telehealth services in their homes—regardless if they live in a rural or urban area.
- However, the HIPAA privacy waivers should not be made permanent. Instead, HHS should be focused on rulemaking that improves care coordination and access (see the Notice of Proposed Rulemaking to modify the HIPAA Privacy Rule (1/21/2021). Congress also needs to enact comprehensive federal privacy legislation covering organizations not specifically covered under other health-related privacy laws and regulations. In addition, the payment parity waivers should not be made permanent as there is little evidence to suggest this kind of parity increased access to digital health services. CMS should explore circumstances in which payment parity may be appropriate.

To promote the consistency, quality and equity of digital health, the federal government should work with industry stakeholders to develop evidence-based guidelines and industry standards regarding the use of digital health.

- It may be difficult for governmental bodies to keep up with all the developments in digital health. Changes occur quickly and technology is constantly evolving.

  For that reason, government organizations should work more closely with industry and health care stakeholders to develop standards and evidence-based guidelines regarding digital health. For example, CTA® is accredited by the American National Standards Institute® as a standards developing organization and is developing standards related to the use of artificial intelligence in areas including health care, mobile health solutions, digital therapeutics and mental health technology.[43] CTA has also published evidence-based guidelines on areas like virtual care and the privacy of personal health data.[44]

  CTA® is not alone. The American College of Cardiology® has created the Applied Health Innovation Consortium to drive thought leadership and evidence for application of artificial intelligence and digital technology in a clinically meaningful way.[45] There are other organizations who are also developing industry-wide consensus standards and guidelines.

  The government should take advantage of this subject matter expertise and find ways to partner with these organizations. Greater government involvement in these efforts will lead to more informed, trustworthy policy decisions that will prove critical when the country tackles the next public health emergency.

Industry stakeholders and associations, in partnership with appropriate governmental bodies (such as the Health Resources and Services Administration), should develop education and training programs for digital health.

- The programs need to: (1) educate consumers about the benefits and limitations of digital health tools and how to maximize them; and (2) train the health care workforce to ensure care providers are sufficiently able to assess, adopt and implement new health technologies into health care services.

We strongly encourage professional clinical schools to establish formal education and training programs and curricula specifically focused on the use of digital health to ensure that the health care workforce of the future is fully prepared with a fundamental understanding of technology to effectively evaluate and appropriately use new technological solutions.

Federal, state and local governments should promote policies that expand access to early detection, screening and clinical interventions enabled by digital health.

Technology is a critical component to making this approach work—and policies that incentivize public/private partnerships among clinicians, hospitals/health systems, payers, the health information technology sector, educators, government agencies and local community institutions will also be important.

Health Data & Privacy

When the COVID-19 pandemic began, health care systems, the federal government and local and state public health authorities tried to leverage existing lines of public health data sharing to track infections, conduct contact tracing efforts, study the nature of the illness and share information about potential effective treatments.

Data Sharing Permissions

Due to varying state laws and technologies implemented by public health agencies, jurisdictions must coordinate with one another to develop frameworks to share data and services. Although there is a national data structure to collect certain information important in a pandemic, such as the number of infections and deaths or hospital capacity, other public health data collection is left to

state and local authorities. This led to jurisdictions developing varied methods for collecting and using public health data. As a result, to standardize data collection during the pandemic, public health agencies had to coordinate with one another on an ad hoc basis and negotiate one-off multi-jurisdictional agreements to collect data.

Some state and local public health laws create difficult requirements agencies must meet before they may disclose information to other parties. In addition, agencies without such legal restriction also developed policies before the pandemic that limited or restricted data sharing in the interest of protecting the privacy of their citizens. In the absence of federal guidelines on data sharing, public health agencies had to develop data policies on-the-go before agreeing to enter into sharing arrangements with other jurisdictions or other parties. In many states and local jurisdictions this meant seeking approval or guidance from their legislatures or governors. This varied process minimized effective coordination and sharing of important public health data.

Arrangements made between public health agencies in different jurisdictions also vary in terms of the level of data integration, ranging from ad-hoc agreements for data sharing to the creation of merged data collection programs to facilitate information sharing and other services.

One particularly concerning example in tracking the country's progress in combating COVID-19 is the lack of interoperability and/or data use restrictions between state immunization registries and the CDC. While the CDC aggregates information on vaccinations across jurisdictions, the dataset has been criticized for missing, latent and inaccurate data. Without the CDC serving as a trusted health information network hub, other jurisdictions and parties must seek to connect individually to obtain data. For one immunization registry to share information with the other registries would require data-sharing agreement with over 60 registries.

To create a national network would require more than 60 registries signing a total of more than 1800 different agreements.[46] This does not even capture the agreements that would have to be entered for other key organizations such as providers and payers to connect with and use the information.

These issues reflect the lack of a robust public health data infrastructure. In a recent report the Congressional Research Service ("CRS") noted that "no federal data collection system for relevant information existed for the pandemic."[47] One study found that 40% of hospitals reported that public health agencies lacked the capacity to receive data electronically.[48] A report from the Office of the National Coordinator for Health Information Technology indicates that in 2019—while the vast majority of non-federal acute care hospitals used certified electronic health record ("EHR") technology—only 55% used the technology to exchange patient data and almost 75% had challenges in electronically exchanging information across different EHR platforms.[49]

The CRS report acknowledged that while there are efforts underway to modernize public health data systems, these efforts are hampered by several challenges, including a lack of standards facilitating data sharing between health care organizations and public health departments.

Governance and Differing State Approaches and Lack of Coordination

HHS has been acting in more of a coordinating role for state and local public health departments during the pandemic response than providing top-down direction. The CDC released non-binding guidance on topics ranging from the use of masks,

social distancing, the length of quarantine following an exposure to COVID-19 and the re-opening of businesses. However, states were never required to adopt or enforce these recommendations. The federal government similarly helped states bid for needed supplies, such as personal protective equipment (PPE) and ventilators.

Contact tracing. As has been the case with so much during the current pandemic, states developed varying approaches to contact tracing. While over 60 countries deployed digital contact tracing apps, only half of U.S. states and territories have made these widely available to their residents. Currently, 25 states and territories have partnered with Apple® and Google® to deploy "Exposure Notifications" with their public health authorities since 2020, for both Android® and iPhone® smartphones.[50] With additional help from Microsoft, the Association for Public Health Laboratories (APHL) hosts a national system to allow exposure notifications to work across state lines (https://www.aphl.org/programs/preparedness/Crisis-Management/COVID-19-Response/Pages/exposure-notifications.aspx). As of May 2021, the majority of these states have enrolled over 15% of their residents, with some states approaching 50%.[51]

There are many reasons for this variation in adoption. Some point to privacy concerns—although Apple® and Google® have made great efforts to assure the public that users must opt-in to use the system, the system doesn't track location, and users can choose whether or not to share their COVID-19 test result.[52] Others point to the lack of a coordinated messaging campaign about contact tracing apps across federal, state and local governments. While research is still ongoing, early analysis estimates that Washington state's exposure notifications deployment prevented about 6000 cases of COVID-19 in just the first 4 months.[53]

Vaccination prioritization. States took different approaches to vaccination prioritization following different CDC prioritization guidelines. Some focused on particular populations and occupations, such as nursing home residents, teachers and first

responders, while others focused on seniors over the age of 65 or those with particular medical conditions. Some states allowed residents of other states to be vaccinated in certain situations (e.g., health care workers that live outside the jurisdiction, but work at a facility within the jurisdiction), while others tried to limit vaccination to residents only. Some states allowed wider distribution outside of the current priority list if the vaccine otherwise would spoil, while other states threatened penalties for vaccinating individuals outside of the current priority list.

States relied on their vaccination distribution data to fine-tune vaccination policies (e.g., fine-tuning vaccination appointment protocols to ensure that vaccines are distributed rapidly and do not spoil) and targeted outreach to certain populations.[54] However, data "blind spots" prevented state and federal officials from understanding why there were gaps between vaccine shipments and distribution (i.e., records of vaccine getting into the arms of people).[55] Better, more consistent data would have helped governments streamline vaccine distribution particularly in the beginning of the vaccination push in the states. These gaps also impacted stakeholders like health insurance providers which conducted significant outreach efforts to enrollees about vaccination but discovered that a significant percentage of those contacted already had been vaccinated.

Such a waste of effort and resources could have been prevented with more comprehensive, accurate and updated data and better access to data by non-

government stakeholders who played a key role in the pandemic response.

Data Silos Preventing Access to Valuable Data by Health Authorities and Preventing Better Coordination Among Sectors

Before HHS created a hub for hospitalization data (the HHS Protect Public Data Hub),[56] it was difficult for public health agencies to get a national picture of hospital staffing, ICU bed availability and the saturation of COVID-19 patients in hospitals.

Researchers had to piece together national data sets from siloed data sources from various state and local agencies and private health data brokers.

The creation of data silos for hospitalization capacity and supplies is understandable given local control and oversight of health care resources. In many ways, state and local governments are better equipped than the federal government to manage a regional response to supply or bed shortages, and most health emergencies are local or regional in nature. Accordingly, states had the freedom to develop innovative approaches to data collection and state and local governments to develop sophisticated and effective reporting systems.

Having national dashboards can help the federal government better coordinate pandemic response by providing the federal government a better sense of the most pressing areas for additional supplies and assistance in expanding health system capacity.[57] The risk of implementing national data collection, however, is that it can create additional burden on key stakeholders—health system administrators and information managers—who may be required to overlay national reporting responsibility onto existing state and local reporting requirements.

It is important to consolidate local, state and national reporting obligations to ease these burdens on health system administrators and information managers.

Non-governmental entities maintain additional local, regional and national data that could be valuable in tackling public health challenges. However, these entities may have proprietary or other commercial interests that discourage them from offering their data to outside researchers or public databases.

Further, individual privacy and security protections can restrict or complicate data sharing. Unless the non-governmental entity includes a statement in its privacy policy that it will share consumer information with public health agencies, consumers may not have prior notice that the data they share with the entity will be used for public health purposes. Stories in newspapers, websites or broadcast media revealing that companies or organizations have contributed identifiable data (or even de-identified data) to public health databases could negatively affect the organization.

Additionally, the Federal Trade Commission ("FTC") has actively used its authority to file complaints against commercial entities that use or disclose consumer information in a manner inconsistent with established privacy policies. Government agencies and non-government organizations must clearly communicate to consumers the benefit of data contributions for public health purposes, and the privacy and security protections in place to prevent misuse of such data.

Lack of Interoperability

A lack of interoperability can prevent public health agencies and other organizations from combining their data, thereby preventing public health agencies from gaining additional insight about infections, treatments and immunizations.

There are two interoperability issues: 1) data collection systems, such as electronic health record systems or immunization information systems, may not be able to export data to another system in a manner that the receiving system can process; and 2) data collection systems that use different documentation styles or data definitions can create a barrier to combining the data.

Organizations that find themselves in the first situation must develop interfaces to facilitate the transfer of data between the data collection systems,

which can be expensive. Organizations in the second scenario may need to hire third-party data aggregators or conduct manual data conversion to "sync up" the data collected between systems so that the data is consistent.

Third parties, such as state health information exchanges and other independent data brokers, have tried to alleviate interoperability issues by providing data aggregation and translation services, facilitating the reporting of consistent data to public health agencies.[58] Additionally, the federal government through the EHR Certification Program has moved to require EHR vendors to offer standardized application programming interfaces ("APIs") to EHR data using the Fast Healthcare Interoperability Resources ("FHIR") standard. By December 31, 2022, these APIs are required to be equipped to, upon demand, export selected data categories about selected patient populations, such as immunizations, medications, laboratory results and conditions.

Eventually, public health authorities may be able to leverage these tools to more easily access EHR data.

Such data aggregators, translation engines and interfaces can only be effective if the potential data submitters are consistently and accurately capturing the data that public health agencies wish to analyze. The simplest way is to ensure that health care providers are capturing the intended information in their typical workflows (or to make it easy for them to do so).

Data Privacy Issues

Unlike other jurisdictions, the United States has adopted a sectoral approach to privacy laws at the federal level. This means that the privacy regulations that apply to data collected in the United States depends on the type and context of the data collected.

Perhaps the most well-known federal privacy law in the health care sector, the Health Insurance Portability and Accountability Act of 1996, applies to "covered entities" and their "business associates." "Covered entities" consist of health insurance providers, health care clearinghouses (entities that assist the submission of claims to health insurance providers) and health care providers.[59] "Business associates" are third parties that create, receive, maintain or transmit protected health information ("PHI") on behalf of covered entities.

However, identifiable health information collected by public health agencies is not protected by HIPAA (unless such health information is collected in the public health agency's capacity as payor).

Covered entities are generally required to obtain written authorization from individuals before using or disclosing their PHI unless an exception applies. Generally, disclosures for "treatment," "payment" and "health care operations" purposes do not require a written authorization. Disclosure of PHI to public health authorities authorized by law to collect such PHI also does not require a written authorization.

Any PHI disclosed to a public health agency must be limited to the "minimum necessary" required for the purpose of the public health agency's authorized information collection. The "minimum necessary" requirement can make disclosures of PHI to public health agencies difficult for covered entities—as they must evaluate what constitutes the minimum necessary and separate the PHI that is not part of the minimum necessary PHI for the disclosure.

Typically, business associates are permitted to disclose PHI only as permitted by their business associate agreements with covered entities.

Business associates cannot disclose PHI for public health purposes unless the covered entity has first agreed to permit the business associate to do so. Recognizing this limitation, OCR, the agency within HHS charged with enforcing HIPAA, instituted a policy to exercise enforcement discretion to permit business associates to make a good faith use of, or disclose, a covered entity's PHI for public health activities during the COVID-19 pandemic.

To take advantage of this flexibility the business associate must inform the covered entity within 10 calendar days of making a disclosure.[60]

There are two other commonly used privacy-protective pathways for covered entities to disclose information to public health agencies under HIPAA. First, covered entities may remove certain identifiers from PHI to render it "de-identified data." There are two ways to turn PHI into de-identified data:

1) by having a statistical expert review the data set or de-identification method and determine that there is a very low risk of re-identification (the "Expert Determination Method") and 2) by removing 18 specific identifiers from the PHI, including any geolocation information smaller than a state and any element of dates relating to the individual smaller than a year (e.g., birth dates or dates of service) (the "Safe Harbor Method").

Although the Safe Harbor method is the quicker and more cost-effective method of de-identification, often entities collecting de-identified data for public health purposes need more granular geolocation information than a zip code or date information shorter than a whole year. In these situations, covered entities and public health departments must determine if they can use the Expert Determination Method or instead make use of the second privacy-protective pathway for public health disclosures—the disclosure of a "limited data set" of PHI.

Under the limited data set pathway, a covered entity may disclose PHI for research, public health, or health care operations purposes if the data has been stripped of all 18 identifiers from the Safe Harbor Method except for town, city, state and zip code and dates relating to the individual (which can remain in the limited data set). To disclose a limited data set, the covered entity must enter into a data use agreement with the recipient that, among other things, prevents further disclosure of the limited data set beyond what is agreed to. The limited data set pathway is helpful for public health disclosures, but still requires the negotiation of a data use agreement, which can take time, particularly if multiple public health agencies are conducting the data collection.[61]

In the European Union, the General Data Protection Regulation ("GDPR") applies more broadly to information collected about residents of the EU.

In addition, states like California have started passing legislation to better protect consumer information. To avoid a situation where organizations need to comply with 50 separate privacy laws, policy makers should enact a more comprehensive federal privacy law in the U.S.

Several different privacy bills have been introduced in the current Congress, but none have passed the chamber in which it was introduced.

Recommendations for Health Data and Privacy

Congress should pass comprehensive federal privacy legislation creating one national standard specifically covering stakeholders not covered by other privacy laws and regulations (e.g., HIPAA). Legislation should balance the need for privacy and security with the need for data mobility and innovation.

We believe that privacy legislation must:

- Provide individuals with transparency about how their health data is collected, used, stored and shared through a privacy policy or other public statement that clearly outlines the organization's policies and practices with respect to the collection, use and disclosure of the data.

- Where practicable, require organizations to provide individuals the ability to access, delete and correct their health data that those companies collect or maintain.
- Clarify that the FTC is the primary enforcing agency for the new law.
- Prohibit organizations from knowingly retaining individuals' health data beyond the time appropriate to provide the expected function or service, unless otherwise agreed to by the individual or required by law.

In partnership with the private sector, the government should develop a national system to collect up-to-date clinical, virological, bacterial and epidemiological information regarding trends in infectious diseases to help project and monitor health care needs during public health emergencies.

- Given how much important data exists outside health care institutional settings—particularly in consumer-facing devices such as data from glucose monitoring devices, digital thermometers, wearables and mobile health applications, to name a few—we believe it is critical that the government develop a comprehensive system to collect certain anonymized health and other data from all sources. This system cannot be developed without significant involvement from private sector organizations which collect such data as part of their normal operations.
- The information should be collected on an individually identifiable level, but only HIPAA covered entities should be able to access the data at that level. All other stakeholders should be given access to anonymized data.
- If a federated system is used, the federal government should establish a network with rules of the road for trusted exchange and common agreement such that entities can be vetted once and access each system.

The federal government should establish a national early warning system based on aggregated data from digital tools, including those used by individuals beyond the confinement of health care facilities, capable of identifying disease hotspots.

- An early-warning system, such as for significant weather events, would allow officials to identify hotspots and initiate earlier interventions to better contain spread of disease. We need a coherent system to use data effectively as a powerful warning system.

Industry stakeholders, in partnership with the federal government, should establish (or harmonize existing) national standards governing minimum requirements for developing datasets and data formats to provide better data consistency.

- Establishing standards will better enable data exchange, data management and data aggregation which will make it easier for organizations like public health authorities and researchers to access and use the data more effectively in response to public health emergencies.

We should encourage greater investment to help develop more open and secure data platforms to facilitate peer-to-peer exchange of health and other information focused on issues such as availability of resources.

- Properly functioning open data platforms can only work if these platforms operate on common interoperability standards and are fully available to health care providers, public health and other government officials and researchers.

Conclusion

The COVID-19 pandemic has been a significant crisis and underscored certain longstanding weaknesses in the U.S. health care system, including overstretched public health agencies, a fragmented public health data infrastructure, fragile supply chains, inequitable care and outdated health-related laws and regulations. The crisis, however, also highlighted opportunities for change regarding how the greater use of digital health and health information technology will help the country better plan for, and respond to, public health emergencies.

Several things will need to change before that promise can be realized. The country's broadband infrastructure will need to be significantly improved. Outdated laws and regulations will need to be modernized as will the country's public health data infrastructure. The lessons learned from the COVID-19 pandemic should spur greater use of digital health and health information technology for improved planning, response, coordination and remediation to effectively respond to future public health emergencies.

References

[1] As of October 1, 2021, there have been almost 5 million deaths worldwide due to COVID-19 based on almost 235 million confirmed cases. The U.S. alone has almost 700,000 deaths and approximately 44 million cases. See COVID-19 Map - Johns Hopkins Coronavirus Resource Center (jhu.edu); COVID-19 Map - Johns Hopkins Coronavirus Resource Center (jhu.edu)

[2] Some researchers, analyzing genome data and using epidemiological simulation, are now estimating that that human-to-human transmission likely stretches back to mid-October to mid-November of 2019 in Hubei Province, China, with a likely short interval before epidemic transmission was initiated. (Timing the SARS-CoV-2 index case in Hubei province | Science (sciencemag.org).

[3] IHR Emergency Committee on Novel Coronavirus (2019-nCoV) (who.int).

[4] https://www.nejm.org/doi/full/10.1056/NEJMoa2001191. Note some researchers believe the coronavirus was circulating in the U.S. as early as December 2019 (https://academic.oup.com/cid/article/72/12/e1004/6012472).

[5] https://www.nytimes.com/article/coronavirus-timeline.html

[6] Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID–19) Outbreak, 85 Fed. Reg. 15,337 (Mar. 18, 2020) (https://www.govinfo.gov/content/pkg/FR-2020-03-18/pdf/2020-05794.pdf). You can find more on all the Medicare waivers by clicking https://www.cms.gov/about-cms/emergency-preparedness-response-operations/current-emergencies/coronavirus-waivers.

[7] https://www.nytimes.com/2020/03/26/health/usa-coronavirus-cases.html

[8] https://www.cdc.gov/training/publichealth101/public-health.html

[9] https://www.cdc.gov/publichealthgateway/publichealthservices/essentialhealthservices.html

[10] Justeen K. Hyde, PhD, Stephen M. Shortell, PhD, MPH, MBA, "The Structure and Organization of Local and State Public Health Agencies in the U.S.: A Systematic Review.

[11] https://fas.org/sgp/crs/homesec/RL31719.pdf

[12] https://www.nap.edu/download/13093. The structure of non-federal public health systems is determined by how state and local health departments are empowered within a state. In states using a centralized approach, state health agencies operate local health departments essentially as local offices of the state agency. In states with a more decentralized approach, local health departments have more authority to act independently. Local departments are usually funded in part via local property taxes.

[13] https://ajph.aphapublications.org/doi/10.2105/AJPH.2020.305709. State legislatures fund local public health, through grants, contracts administered by the state health agency, general state fund support and other dedicated revenue. The federal government also supports a few very large local governments (e.g., New York City) directly with grants or through funding to state health departments who then

[14] https://www.congress.gov/117/bills/hr1319/BILLS-117hr1319enr.pdf

[15] https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.

[16] https://shop.cta.tech/collections/Research/products/the-future-of-telehealth-and-remote-patient-monitoring-in-the-age-of-covid-19?_ga=2.24669304.319448750.1620256993-1443382493.1533056753. *see also* https://www.cdc.gov/mmwr/volumes/69/wr/mm6943a3.htm.

[17] https://shop.cta.tech/collections/Research/products/the-future-of-telehealth-and-remote-patient-monitoring-in-the-age-of-covid-19?_ga=2.24669304.319448750.1620256993-1443382493.1533056753; *see also* https://www.cdc.gov/mmwr/volumes/69/wr/mm6943a3.htm.

[18] https://www.kff.org/medicare/issue-brief/medicare-and-telehealth-coverage-and-use-during-the-covid-19-pandemic-and-options-for-the-future/

[19] https://www.nature.com/articles/s41591-020-1011-4.pdf

[20] https://www.ccjm.org/content/early/2020/06/08/ccjm.87a.ccc028; https://erj.ersjournals.com/content/early/2021/03/25/13993003.00636-2021

[21] https://www.whatsapp.com/coronavirus/who; https://www.who.int/news-room/feature-stories/detail/who-launches-a-chatbot-powered-facebook-messenger-to-combat-covid-19-misinformation.

[22] *See, e.g.,* https://healthitanalytics.com/news/using-an-ai-powered-chatbot-to-meet-patient-needs-during-covid-19

[23] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7979170/. For a good example of the use of a wearable, please click on https://www.si.com/nba/2020/07/01/oura-ring-nba-restart-orlando-coronavirus.

[24] https://www.jmir.org/2021/2/e25682/

[25] https://covid19.who.int/

[26] https://www.arcgis.com/apps/dashboards/bda7594740fd40299423467b48e9ecf6

[27] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7799428/

[29] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7186767/#:~:text=It%20is%20concluded%20that%20AI,and%20rigorous%20human%2DAI%20interaction.; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7811949/; https://innovations.bmj.com/content/7/2/387.But see, https://www.medrxiv.org/content/10.1101/2020.10.28.20219816v3; https://www.semanticscholar.org/paper/Artificial-Intelligence-and-Coronavirus-COVID-19%3A-Al-Hashimi-Hamdan/836ea7bac13294ee495ff2dc48fe1ad35f8efb3f.

[30] https://www.cms.gov/files/document/summary-covid-19-emergency-declaration-waivers.pdf (pursuant to authority granted under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act).

[31] Coronavirus Preparedness and Response Supplemental Appropriations Act of 2020 (Supplemental Appropriations Act), Section 102; CARES Act Section 3703; see also CMS, Frequently Asked Questions available at https://www.cms.gov/files/document/medicare-telehealth-frequently-asked-questions-faqs-31720.pdf.

[32] The current list of services that may be delivered via telehealth is located at: https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes.

[33] CMS Interim Final Rules, 85 C.F.R. 19230 (April 6, 2020) and 85 C.F.R. § 27550 (May 8, 2020).

[34] 85 C.F.R. § 27550 at 27590.

[35] *Id*.

[36] https://www.cms.gov/newsroom/press-releases/cms-announces-comprehensive-strategy-enhance-hospital-capacity-amid-covid-19-surge.

[37] https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (March 17, 2020).

[38] The announcement is available on the DEA's COVID-19 Information page at https://www.deadiversion.usdoj.gov/coronavirus.html.

[39] The Federation of State Medical Boards has tracked state licensing flexibilities at the following site: https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf.

[40] See, e.g., AAMC Telehealth Competencies, available at: https://www.aamc.org/data-reports/report/telehealth-competencies.pdf; AMA self-paced ME on how to use digital tools: https://edhub.ama-assn.org/pages/telemedicine-cme-course.

[41] https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2020.305784.

[42] https://blogs.microsoft.com/on-the-issues/2019/04/08/its-time-for-a-new-approach-for-mapping-broadband-data-to-better-serve-americans/

[43] https://shop.cta.tech/collections/standards/health-and-fitness; https://shop.cta.tech/collections/standards/artificial-intelligence

[44] https://shop.cta.tech/collections/standards/products/guiding-principles-on-virtual-care

[45] https://www.acc.org/About-ACC/Innovation/ACC-Applied-Health-Innovation-Consortium

[46] https://www.usatoday.com/story/news/health/2020/06/12/coronavirus-vaccine-state-immunization-registries/5321892002/

[47] https://crsreports.congress.gov/product/pdf/R/R46588

[48] https://academic.oup.com/jamia/article/27/8/1306/5842141

[49] https://www.healthit.gov/sites/default/files/page/2021-03/Hospital%20Use%20of%20Certified%20HIT_Interop%20v10_1.pdf.

[50] https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/.

[51] https://www.technologyreview.com/2021/06/16/1026255/us-digital-contact-tracing-exposure-notification-analysis/.

[52] https://www.google.com/covid19/exposurenotifications/.

[53] https://www.doh.wa.gov/Newsroom/Articles/ID/2827/Researchers-from-UW-and-DOH-find-WA-Notify-exposure-notification-tool-is-saving-lives.

[54] https://www.northjersey.com/story/news/bergen/garfield/2021/05/03/garfield-passaic-nj-among-cities-lowest-covid-vaccination-rates/4930962001/

[55] https://khn.org/news/article/huge-gaps-in-vaccine-data-make-it-next-to-impossible-to-know-who-got-the-shots/

[56] https://protect-public.hhs.gov/

[57] https://www.beckershospitalreview.com/data-analytics/covid-tracking-project-co-founder-urges-biden-administration-to-keep-hhs-hospital-data-reporting-system.html

[58] https://www.fiercehealthcare.com/tech/industry-voices-3-ways-health-information-exchanges-have-ushered-a-new-era-by-evolving-their

[59] Note that while most healthcare providers are "covered entities", there are healthcare providers that are not "covered entities" because HIPAA only applies to healthcare providers that engage in standardized electronic transactions. While every healthcare provider that accepts payment from health insurance providers will engage in these transactions, some healthcare providers only accept patients that will self-pay.

[60] 85 Fed. Reg. 19392 (April 7, 2020).

[61] HIPAA does not preempt any federal or state privacy laws that are more stringent in their protection of PHI. As a result, there is a patchwork of state laws that covered entities must navigate before disclosing PHI to public health agencies. Many of these state laws are concern sensitive categories of treatment information, such as mental health, substance use disorder, and sexually transmitted diseases. Many of these state laws include exceptions that permit disclosures to public health agencies without first obtaining written consent from the patient. However, some industry stakeholders hold misperceptions about whether they may pursue certain uses and disclosures of health information under state and federal laws and encounter differing interpretations as they seek to comply with and implement pathways available under such laws. Together, these misperceptions and ambiguities undermine efforts to understand whether additional restrictions on the permissible use and disclosure of health information are necessary and appropriate to adequately protect patients' rights and welfare. Notably, some of the more stringent state and federal privacy laws limit public health organizations from re-disclosing sensitive categories of information. This helps to assure patient privacy but prevents public health agencies from readily sharing the information with researchers and other third parties.

For more information please contact:
Rene Quashie, Vice President, Policy & Regulatory Affairs,
Digital Health at **membership@CTA.tech**.