CONFIDENTIALITY
COALITION

General Committee Meeting
Thursday, October 15, 2020
3:00pm – 4:00pm

Zoom Link: https://zoom.us/j/99433455444?pwd=c0RsczQ3REl2RnM1WkJnN1MxSzRHQT09
Phone Number: 301-715-8592
Meeting ID: 994 3345 5444
Password: 482315

1. Welcome and Introductions

2. Guest Speaker: Health Information Technology Survey — Attachment 1, 2
   Ben Moscovitch, Molly Murray, Ashley Ashworth, The Pew Charitable Trusts

3. Regulatory Update
   a. HIPAA Coordinated Care Proposed Rule
   b. ONC Information Blocking Interim Final Rule

4. Legislative Update — Attachment 3, 4, 5
   a. Improving Medicaid Programs' Response to Overdose Victims and Enhancing (IMPROVE) Addiction Care Act
   b. Senate Privacy Legislation
   c. Energy & Commerce GAO Cybersecurity Request

5. TCPA Update — Attachment 6

6. Monthly Privacy Round-Up — Attachment 7

7. Articles of Interest — Attachment 8, 9, 10, 11

Attachment #1

The Pew Charitable Trusts – Health Information Technology Bios

Ben Moscovitch directs Pew's efforts to improve the safety of electronic health records and enhance the exchange of information, so health care providers and patients have the data they need to make informed decisions. This work will help advance efforts to ensure that the design, implementation, and use of EHRs do not contribute to unintended harm, and that they can be used to improve care. Previously, Moscovitch worked on Pew's medical devices project, advancing policy reforms to support innovation, patient safety, and quality improvement. Before joining Pew, Moscovitch was a public policy communications officer for the National Association of Chain Drug Stores. He also previously worked as a journalist, covering medical product regulation and legislation. Moscovitch received a bachelor's degree in English from Georgetown University and master's in Middle Eastern history from Tel Aviv University.

Molly Murray is an Officer on Pew's health information technology team. Her work focuses on patient matching, or correctly linking patients between disparate health IT systems, to ensure providers have complete data to make informed care decisions. Before joining Pew, Murray worked as the Senior Health IT and Quality Specialist at the American College of Surgeons. She previously worked in health IT implementation, both in electronic health records and in data analytics platforms. She holds a bachelor's degree in Political Science from the University of Massachusetts, Amherst and a master's in public administration from the University of North Carolina, Chapel Hill.

Ashley Ashworth is a Senior Associate with Pew's Health Information Technology project. She works to improve data exchange in health care settings. Prior to joining Pew, she worked at the Trust for America's Health, the Rails-to-Trails Conservancy, and the United States Senate. She received a master's in health science from the Johns Hopkins Bloomberg School of Public Health and a bachelor's degree in health psychology from Andrews University.

Attachment #2

THE PEW CHARITABLE TRUSTS

Patient Priorities on Health Data Access, Sharing, and Patient Matching

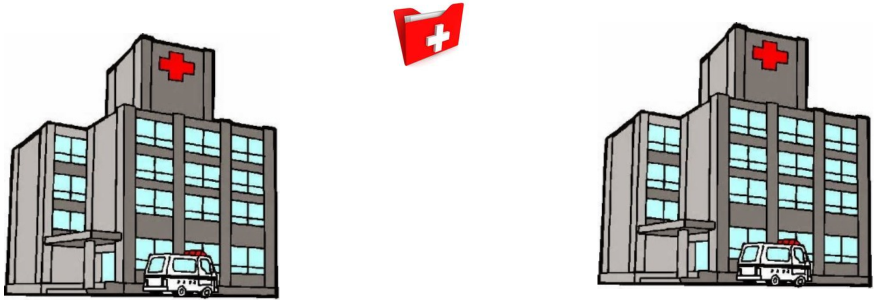
Ben Moscovitch, Ashley Ashworth, and Molly Murray

October 15, 2020

Attachment #2

The Pew Charitable Trusts

Patient safety



Interoperability

Attachment #2

Who we are

Ben Moscovitch

Project Director

Ashley Ashworth

Senior Associate

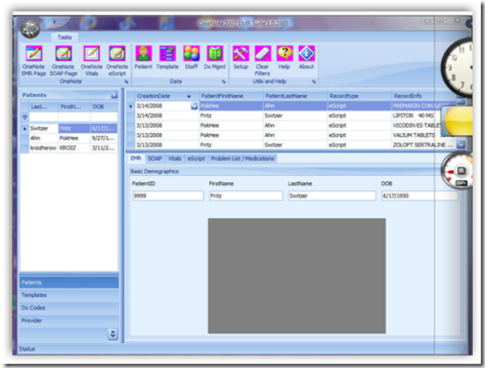
Molly Murray

Officer

Attachment #2

Setting the Stage

- Goal of EHRs- improve care



Patients

Last...	FirstN...	DOB
Switzer	Fritz	6/17/1...
Ahn	PokHee	9/27/1...
kroizherow	KROIZ	3/11/2...

CreationDate	PatientFirstName	PatientLastName	Recordtype	RecordInfo
3/14/2008	PokHee	Ahn	eScript	PREMARIN CONJUGAT
3/14/2008	Fritz	Switzer	eScript	LIPITOR 40 MG
3/13/2008	PokHee	Ahn	eScript	VICODIN ES TABLET
3/13/2008	PokHee	Ahn	eScript	VALIUM TABLETS
3/13/2008	Fritz	Switzer	eScript	ZOLOFT SERTRALINE ...

Basic Demographics

PatientID	FirstName	LastName	DOB
9999	Fritz	Switzer	6/17/1950

- 2016: 21st Century Cures
  - New regulations

Attachment #2

Policymakers address challenges

- 21st Century Cures and associated rulemaking
  - More standardized data for patients and providers
  - Advancing application programming interfaces (APIs)
  - More demographics for patient matching
- Renewed interest in removing federal ban on a unique patient identifier

Attachment #2

Objectives

Understand individual perceptions about…

Patient access to data

Exchange of health data

Privacy

Patient matching solutions

Attachment #2

Methodology

- Public Opinion Strategies and Hart Research Associates conducted a national survey from June 1- July 3, 2020.
- N=1,213 adults ages 18 or older (N=110 by phone and N=1,103 by web).
- Interviews were conducted in English and Spanish
- The survey was conducted using NORC at the University of Chicago's AmeriSpeak panel. AmeriSpeak is a nationally representative, probability-based panel of the U.S. household population.

Attachment #2

Patient Access

- A majority (61%) of adults say they would want to be able to download their EHR to different health apps.
- Younger adults are more interested in downloading. 67% of Millennials compared to 53% of Boomers.
- Education also a factor. 76% of post grads compared to 52% of those with a high school education.
- Surprisingly, chronic health and caregiver status not factors.

Attachment #2

Benefits Outweigh Risks

The health benefits outweigh the privacy risks	32%
The privacy risks outweigh the health benefits	18%
The benefits and risks are equal	28%
The benefits and risks are unclear	21%

Attachment #2

Concerns about HIPAA

How concerned, if at all, would you be about the privacy of your medical information and data if you download it to different health apps you selected to use on your smart phone, computer or tablet?

Extremely/Very Concerned	**35%**
Extremely Concerned	**16%**
Very Concerned	**19%**
Somewhat Concerned	**44%**
Total Not Concerned	**20%**
Not Too Concerned	**16%**
Not At All Concerned	**4%**

And how concerned, if at all, would you be about the privacy of your medical information and data if you found out that once it is downloaded to some health apps it may ***NO LONGER BE PROTECTED BY FEDERAL LAWS RELATING TO PRIVACY SUCH AS HIPAA*** *and may instead be subject to the health app's privacy policy or terms of service?*

Extremely/Very Concerned	**62%**
Extremely Concerned	**42%**
Very Concerned	**20%**
Somewhat Concerned	**28%**
Total Not Concerned	**10%**
Not Too Concerned	**6%**
Not At All Concerned	**4%**

Attachment #2

Provider approval helps

Unapproved apps	Approved by and independent certification board	Approved and recommended by your providers
Total comfortable: 15% Total uncomfortable: 84%	Total comfortable: 61% Total uncomfortable: 39%	Total comfortable: 76% Total uncomfortable: 23%

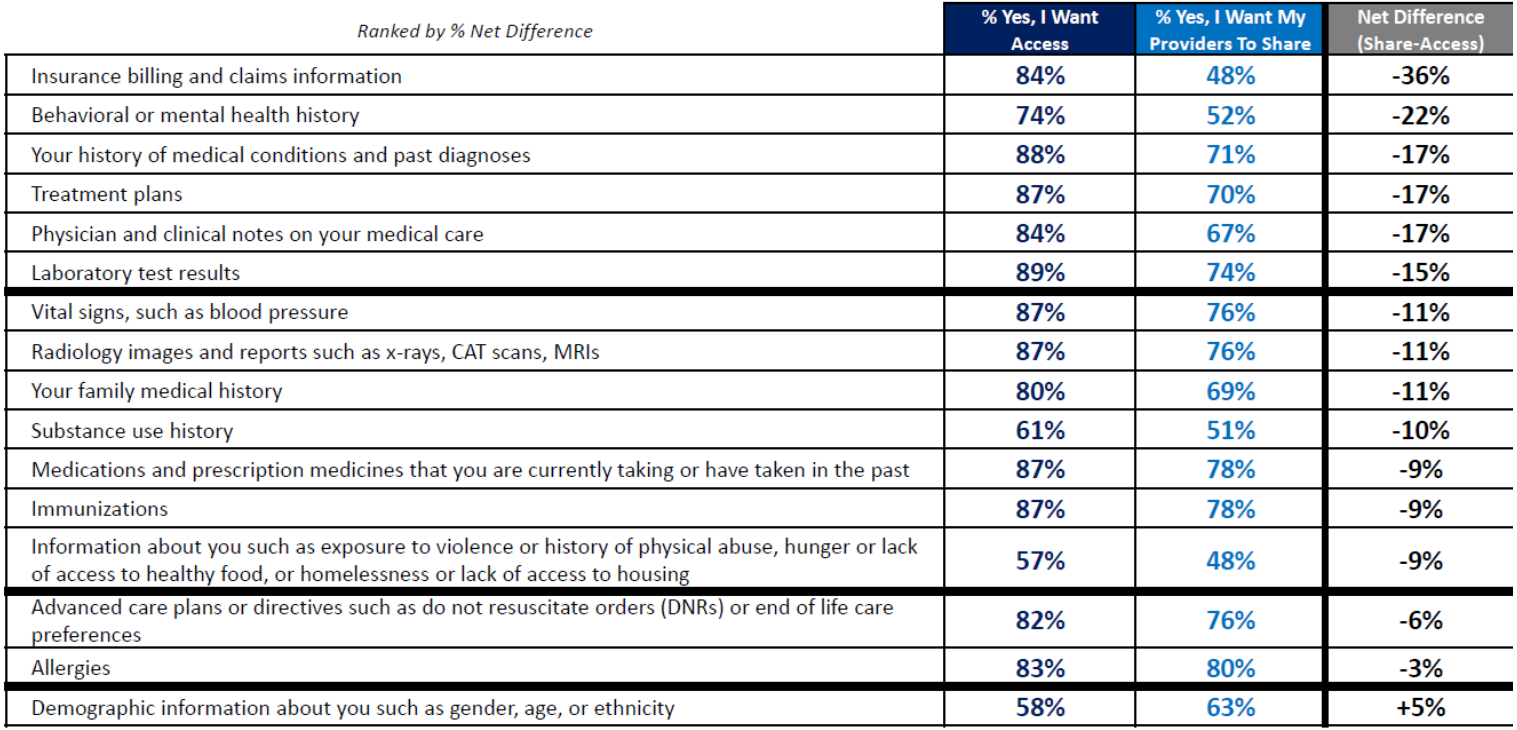
Attachment #2

Provider Exchange

- More than 8 in 10 adults support enabling health care providers to share patient health information between their EHR systems when treating/caring for the same patient.
- Concerns specific to: insurance billing/claims information, mental health or substance use histories, or social determinants of health.

Attachment #2

Access vs Exchange

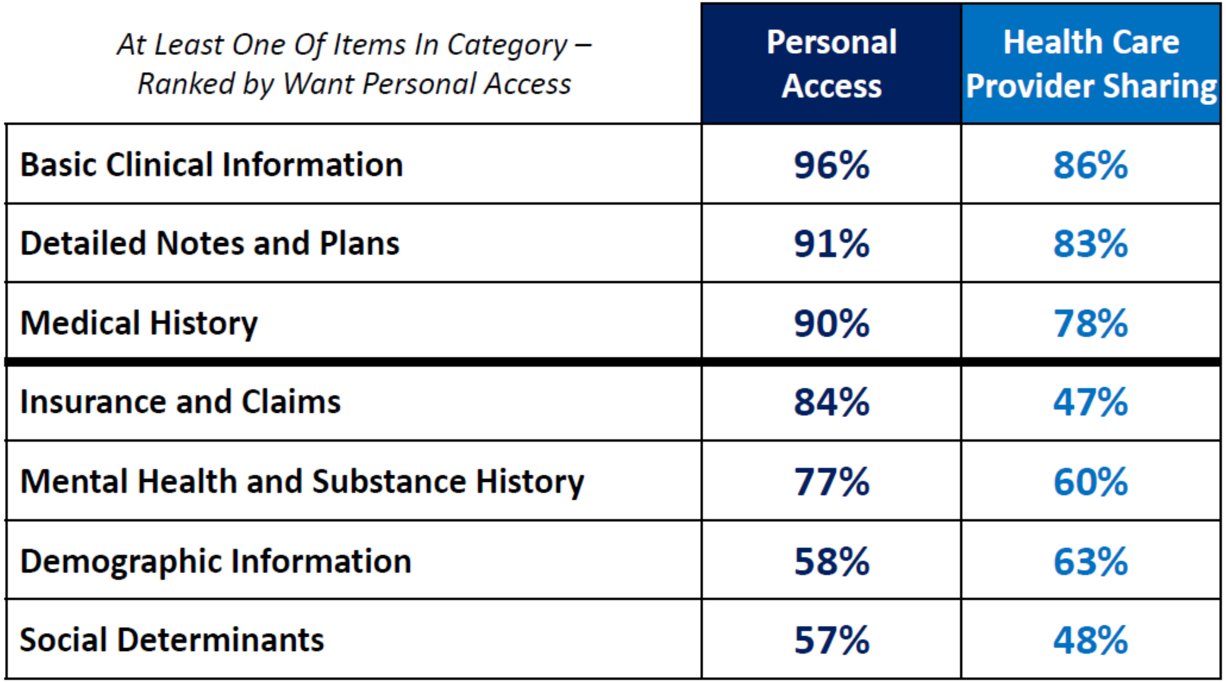


Ranked by % Net Difference

	% Yes, I Want Access	% Yes, I Want My Providers To Share	Net Difference (Share-Access)
Insurance billing and claims information	84%	48%	-36%
Behavioral or mental health history	74%	52%	-22%
Your history of medical conditions and past diagnoses	88%	71%	-17%
Treatment plans	87%	70%	-17%
Physician and clinical notes on your medical care	84%	67%	-17%
Laboratory test results	89%	74%	-15%
Vital signs, such as blood pressure	87%	76%	-11%
Radiology images and reports such as x-rays, CAT scans, MRIs	87%	76%	-11%
Your family medical history	80%	69%	-11%
Substance use history	61%	51%	-10%
Medications and prescription medicines that you are currently taking or have taken in the past	87%	78%	-9%
Immunizations	87%	78%	-9%
Information about you such as exposure to violence or history of physical abuse, hunger or lack of access to healthy food, or homelessness or lack of access to housing	57%	48%	-9%
Advanced care plans or directives such as do not resuscitate orders (DNRs) or end of life care preferences	82%	76%	-6%
Allergies	83%	80%	-3%
Demographic information about you such as gender, age, or ethnicity	58%	63%	+5%

Attachment #2

Broad support for at least some

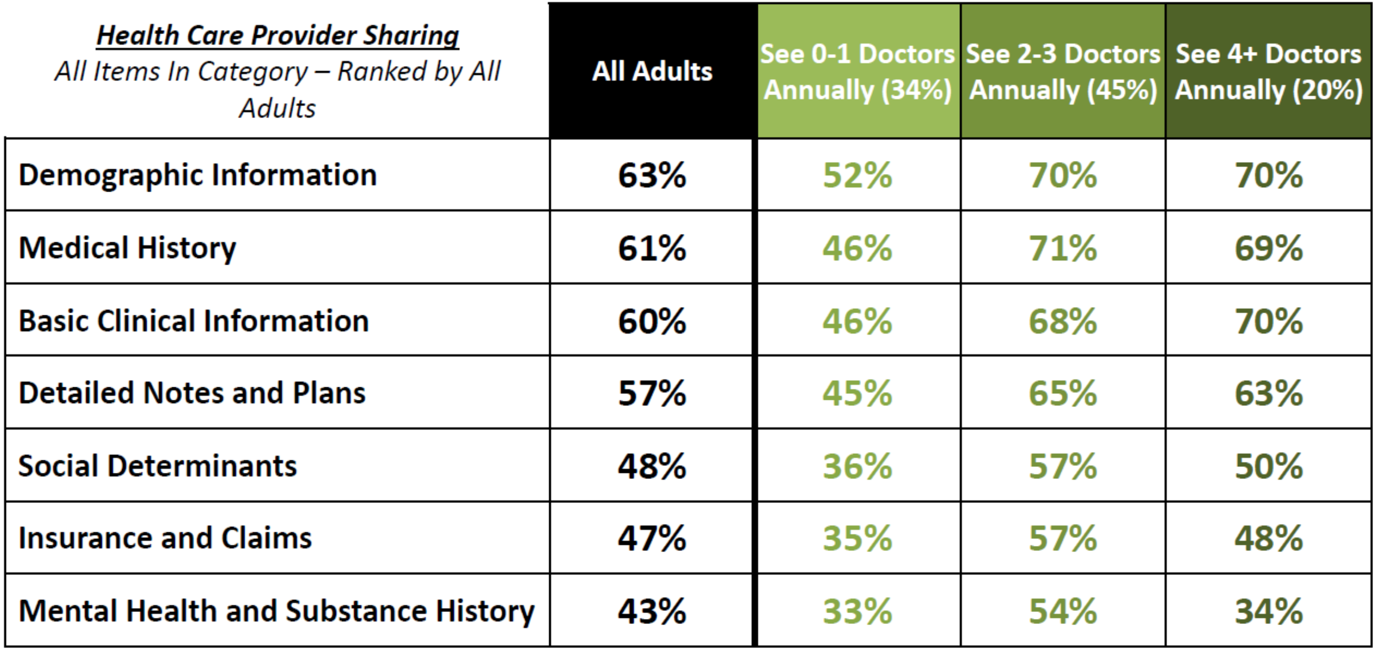


At Least One Of Items In Category – Ranked by Want Personal Access	Personal Access	Health Care Provider Sharing
Basic Clinical Information	**96%**	**86%**
Detailed Notes and Plans	**91%**	**83%**
Medical History	**90%**	**78%**
Insurance and Claims	**84%**	**47%**
Mental Health and Substance History	**77%**	**60%**
Demographic Information	**58%**	**63%**
Social Determinants	**57%**	**48%**

Attachment #2

Frequent users more

Sl



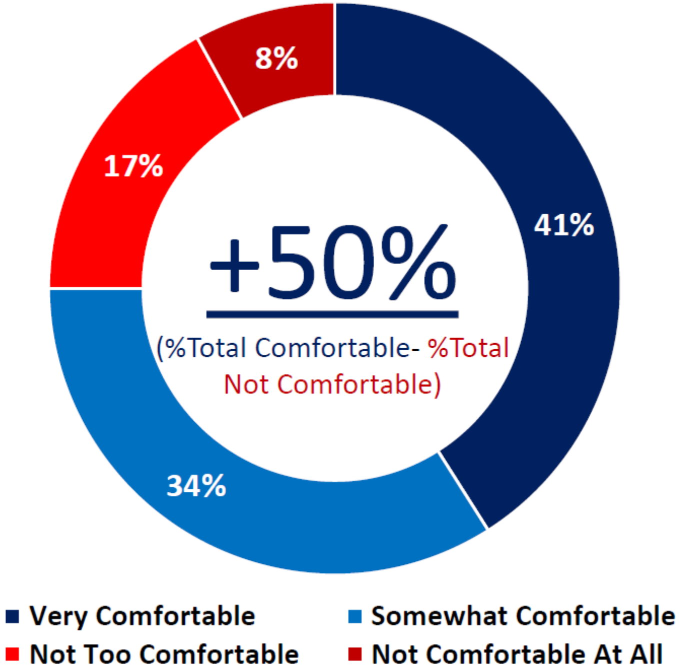
Health Care Provider Sharing *All Items In Category – Ranked by All Adults*	All Adults	See 0-1 Doctors Annually (34%)	See 2-3 Doctors Annually (45%)	See 4+ Doctors Annually (20%)
Demographic Information	63%	52%	70%	70%
Medical History	61%	46%	71%	69%
Basic Clinical Information	60%	46%	68%	70%
Detailed Notes and Plans	57%	45%	65%	63%
Social Determinants	48%	36%	57%	50%
Insurance and Claims	47%	35%	57%	48%
Mental Health and Substance History	43%	33%	54%	34%

Attachment #2

Collection of SDOH

How comfortable would you be with providing your doctor with the following types of information about you for them to enter into your electronic health record: exposure to violence or history of physical abuse, hunger or lack of access to healthy food, or homelessness or lack of access to housing?

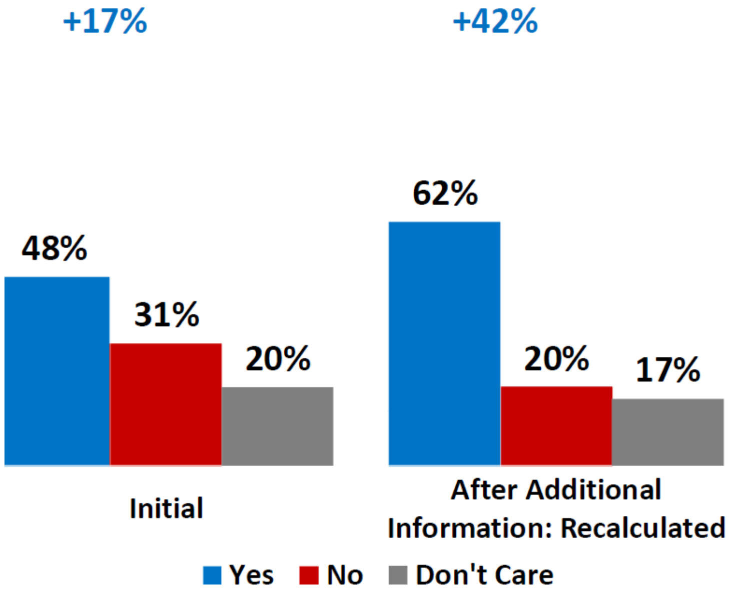
Total Comfortable	**75%**
Total Not Comfortable	**25%**



Attachment #2

Sharing of SDOH

- Hesitation around sharing- only 48% comfortable initially
- Education helps! When told about the benefits of SDOH, comfort increased 14%
- Comfort increases with education and income



Attachment #2

Privacy Concerns

Top reasons for concern:

- Identity theft/blackmail
- Discrimination
- Health apps not covered by HIPAA
- Do not want information shared with tech companies, ie Facebook or Google

TEACHPRIVACY
PRIVACY POLICY
We don't really know what data about you we have or what we're doing with it. When we figure all this out, we'll let you know.
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

Attachment #2

APIs: What's next?

Patients want access to their data

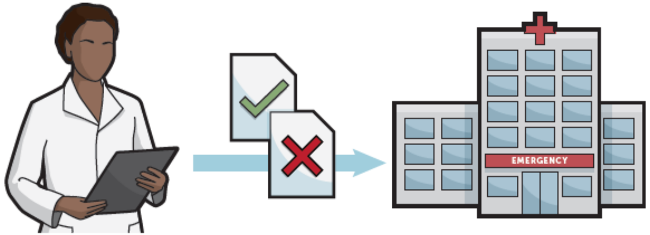
Want providers to be able to communicate

Need privacy solutions

Attachment #2

Patient matching

Patient matching is the ability to accurately link each individual’s records from multiple doctors’ offices or hospitals.



Up to half of patient records are not matched in transfers—e.g., from a rural doctor to an urban hospital.[2]

Attachment #2

Patient matching: Opportunities

- Universal Patient Identifier
- ONC Report to Congress

Attachment #2

Set national standards

Would you support or oppose the federal government setting national standards to more accurately match up a patient's electronic health records across multiple providers?

Total Support:

74%

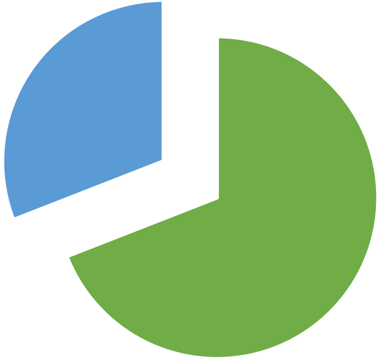
Total Oppose:

25%

Attachment #2

Spend federal money

2/3 support spending federal money to improve patient matching



Even when broken down by political party, there is majority support:

Republicans (total support): **51%**

Independents (total support): **66%**

Democrats (total support): **82%**

THE PEW CHARITABLE TRUSTS

pewtrusts.org

Attachment #2

When asked to choose which one method they would most want to see implemented, scanning a patient's fingerprint is the top choice for the majority of adults.

Total Biometric*	
54% First Choice	69% Combined Choice

Ranked by 1st Choice	First Choice	Combined Choice
Scanning your fingerprint	37%	54%
Assigning a unique number or code to each individual patient which the patient would need to remember or bring with them	22%	41%
Scanning your eye	10%	27%
Using your smart phone or a smart phone app	10%	23%
Comparing photos of your face that your health care providers have taken	7%	18%
Do not support any of these being implemented	13%	N/A

**Total Biometric defined as: scanning fingerprint, scanning eye, and comparing photographs of face*

Attachment #2

Patient matching: What's next?

Americans want this issue solved

Do not support the current spending ban

Supported methodologies should be part of ONC report

Attachment #2

Thank you!

For additional questions or information, please contact:

Ben Moscovitch
Project Director
Health Information Technology
The Pew Charitable Trusts
e: bmoscovitch@pewtrusts.org
@benmoscovitch

Ashley Ashworth
Senior Associate
Health Information Technology
The Pew Charitable Trusts
e: aashworth@pewtrusts.org
@ashleyEashworth

Molly Murray
Officer
Health Information Technology
The Pew Charitable Trusts
e: mmurray@pewtrusts.org

Attachment #3

Improving Medicaid Programs' Response to Overdose Victims and Enhancing (IMPROVE) Addiction Care Act

In 2017, nearly one million nonfatal overdoses were treated in United States emergency rooms, 40 percent of which involved the presence of an opioid.[1] Nonfatal overdoses are one of the most significant predictors of a future overdose.[2]

Medicare and Medicaid have paid for 62 percent of all opioid-related hospitalizations,[3] but Medicaid programs in particular need to institute reforms to meaningfully help enrollees who are battling addiction. A recent study of 3,606 Medicaid-enrolled adolescents (ages 13-22) who experienced an opioid-related overdose found that ***only one in 54 received medication-assisted treatment and less than one in three received any treatment whatsoever.***[4]

Equally concerning, ***Medicaid beneficiaries often continue receiving legal opioid prescriptions even after suffering a nonfatal, opioid-related overdose.*** Approximately 60 percent of Pennsylvania Medicaid beneficiaries who suffered a nonfatal overdose between 2007 and 2013 received another legal opioid analgesic prescription within six months.[5] Boston University and Harvard Medical School found that 91 percent of patients who suffered an opioid-related overdose between 2000 and 2012 received another legal opioid prescription within a year.[6]

In 2018, Congress included a provision (Section 2006) in the *SUPPORT for Patients and Communities Act* (P.L. 115-271) that ensures prescribers are aware of their Medicare Part D patients' history of nonfatal, opioid-related overdoses. ***Unfortunately, this issue was not addressed for Medicaid beneficiaries.***

The *IMPROVE Addiction Care Act* would require that state Medicaid programs use their existing drug utilization review (DUR) programs to identify and assist beneficiaries who have experienced a nonfatal, opioid-related overdose. Specifically, the bill requires that states use DUR programs to:

- ***Connect survivors to treatment*** by identifying individuals who have suffered a nonfatal, opioid-related overdose within the last five years and connect these individuals to effective treatments;
- ***Ensure that prescribers are alerted*** to their patient's previous nonfatal, opioid-related overdose or diagnosis of opioid use disorder;
- ***Make providers aware of fatalities*** if their patient suffers an opioid-related overdose death; and
- ***Perform ongoing reviews*** through retrospective DUR and offer provider education regarding appropriate prescribing practices.

[1] Stephen Liu, Lawrence Scholl, Brooke Hoots, Puja Seth, *"Nonfatal Drug and Polydrug Overdoses Treated in Emergency Departments — 29 States, 2018–2019,"* Centers for Disease Control and Prevention, August 28, 2020, https://www.cdc.gov/mmwr/volumes/69/wr/mm6934a1.htm?s_cid=mm6934a1_w#T1_down
[2] Mark Stoove, Paul Dietze, Damine Jolley, *"Overdose deaths following previous non-fatal heroin overdose: Record linkage of ambulance attendance and death registry data,"* Drug and Alcohol Review, July, 06, 2009, https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1465-3362.2009.00057.x
[3] Pamela Owens, Marguerite Barrett, Audrey Weiss, Raynard Washington, Richard Kronick, "Hospital Inpatient Utilization Related to Opioid Overuse Among Adults, 1993-2012," AHRQ, August, 2014, https://www.hcup-us.ahrq.gov/reports/statbriefs/sb177-Hospitalizations-for-Opioid-Overuse.jsp
[4] Rachel Alinsky, Bonnie Zima, Jonathan Rodean, et al., "Receipt of Addiction Treatment After Opioid Overdose Among Medicaid-Enrolled Adolescents and Young Adults," JAMA Pediatrics, January 6, 2020, https://jamanetwork.com/journals/jamapediatrics/article-abstract/2758103
[5] Winfred Frazier, Gerald Cochran, Wei-Hsuan Lo-Ciganic, et al., *"Medication-Assisted Treatment and Opioid Use Before and After Overdose in Pennsylvania Medicaid,"* JAMA, August 22, 2019, https://jamanetwork.com/journals/jama/fullarticle/2649173
[6] Marc Larochelle, Jane Liebschutz, Fang Zhang, Dennis Ross-Degnan, Frank Wharam, *"Opioid Prescribing After Nonfatal Overdose and Association With Repeated Overdose,"* Annals of Internal Medicine, January 5, 2016, https://www.acpjournals.org/doi/10.7326/M15-0038

Attachment #4

116TH CONGRESS
2D SESSION

S. ______

To amend title XIX of the Social Security Act to encourage appropriate prescribing under Medicaid for victims of opioid overdose.

IN THE SENATE OF THE UNITED STATES

Mr. TOOMEY (for himself and Mr. MANCHIN) introduced the following bill; which was read twice and referred to the Committee on ______________

A BILL

To amend title XIX of the Social Security Act to encourage appropriate prescribing under Medicaid for victims of opioid overdose.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ‘‘Improving Medicaid Programs’ Response to Overdose Victims and Enhancing Addiction Care Act’’ or the ‘‘IMPROVE Addiction Care Act’’.

SEC. 2. ENCOURAGING APPROPRIATE PRESCRIBING UNDER MEDICAID FOR VICTIMS OF OPIOID OVERDOSE.

(a) IN GENERAL.—Section 1927(g)(2) of the Social Security Act (42 U.S.C. 1396r–8(g)(2)) is amended by adding at the end the following new subparagraph:

"(E) ADDITIONAL DRUG USE REVIEW REQUIREMENTS.—As part of a State's prospective and retrospective drug use review under subparagraphs (A) and (B), as applicable, the State shall, not later than January 1, 2022, develop and implement, or review and update, protocols to, subject to any applicable privacy or confidentiality protections—

"(i) identify individuals receiving benefits under this title who have experienced a nonfatal opioid-related overdose within the last 5 years, to the extent that such data is available, and make a good faith effort to connect these individuals to treatment options that have been determined appropriate by the Secretary;

"(ii) if an individual receiving benefits under this title experiences a fatal overdose that is opioid-related (or, if specified by the Secretary, related to another covered outpatient drug), not later than 6 months after the date of such overdose—

“(I) notify each provider that, during the period (to be established by the Secretary) preceding such overdose, prescribed opioids (or such other specified covered outpatient drug, if applicable) to such individual of such overdose; and

“(II) provide each such provider with educational materials on prescribing opioids (or such other specified covered outpatients drugs, if applicable);

“(iii) ensure that a provider who is treating an individual receiving benefits under this title has notice of the individual’s diagnosis or history of opioid use disorder, opioid poisoning diagnosis, or history of nonfatal opioid-related overdose; and

“(iv) perform ongoing retrospective drug utilization reviews and offer provider education that is informed by such reviews (which may include education provided under an educational outreach program established under subparagraph (D) or through an intervention described in paragraph (3)(C)(iii)) regarding appropriate prescribing practices for individuals receiving benefits under this title with a diagnosis or history of opioid use disorder, a history of nonfatal opioid-related overdose, or an opioid poisoning diagnosis.''.

(b) TECHNICAL AMENDMENTS.—Section 1932(i) of the Social Security Act (42 U.S.C. 1396u–2(i)) is amended—

(1) by striking ''section 483.3(s)(4)'' and inserting ''section 438.3(s)(4)''; and

(2) by striking ''483.3(s)(5)'' and inserting ''438.3(s)(5)''.

Attachment #5

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

GREG WALDEN, OREGON
RANKING MEMBER

ONE HUNDRED SIXTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

October 9, 2020

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

The Department of Health and Human Services (HHS) is the primary agency responsible for protecting public health and providing essential human services, especially for those who are least able to help themselves. The Department works closely with state, local, tribal, and territorial governments to administer more than 300 programs covering a wide spectrum of activities and healthcare services, many of which involve the collection of sensitive data.

HHS relies extensively on information systems and networks to conduct operations, process transactions, account for assets, deliver goods and services to constituents, and communicate with individuals and other organizations. In doing so, HHS information systems collect, process, and maintain highly sensitive information including proprietary business information, public health records, and personally identifiable information. Such information is used to deliver goods and services to beneficiaries of the agency's programs. Thus, a disruption in the information systems owned and operated by HHS could be catastrophic for the many Americans that rely on its goods and services. Given this, it is important that HHS implements protections to secure its information systems and provides ongoing assistance to address emerging cybersecurity threats across the agency.

In addition, as HHS and its component agencies are engaged in the nation's efforts to respond to and recover from the Coronavirus Disease of 2019 (COVID-19) pandemic, the agency has faced an increase in various cyber-based threats to its information systems and data. These incidents and others like them, pose a serious challenge to the agency's ongoing efforts to provide timely services during the COVID-19 pandemic. As such, protecting HHS computing operations during the pandemic response is paramount to the nation's security, economic well-being, and public trust.

Attachment #5

The Chief Information Security Officer at HHS recently acknowledged that the ongoing COVID-19 public health crisis has placed a new target on HHS, and malicious actors have boosted their efforts to infiltrate the agency and access sensitive data.[1] In addition, it was reported in March 2020 that HHS suffered a cyber-attack on its computer system. According to people familiar with the incident, it was part of a campaign of disruption and disinformation that was aimed at undermining the response to the coronavirus pandemic and may have been the work of a foreign actor.[2] Further, emerging cyber threats, such as the advanced persistent threat groups that exploited COVID-19 in early 2020, underscore the importance of effectively protecting information systems supporting the agency.

Given the types of information created, stored, and shared on the information systems owned and operated by HHS, it is important that the agency implement effective incident response handling processes and procedures to address persistent cyber-based threats. Based on the agency's expressed concern and recent past incidents, we would request that the GAO evaluate HHS's incident response capabilities. This should include assessing the agency's forensic threat intelligence data infrastructure used in responding to major or significant incidents involving persistent threats and data breaches.

Thank you for your prompt attention to this request. Please work with Kevin McAloon of the Majority Committee staff at (202) 225-2927 and Alan Slobodin of the Minority Committee staff at (202) 225-3641 on the specifics of your evaluation.

Sincerely,

Frank Pallone, Jr.

Frank Pallone, Jr.
Chairman

Greg Walden

Greg Walden
Ranking Member

Diana DeGette

Diana DeGette
Chair
Subcommittee on Oversight
and Investigations

Brett Guthrie

Brett Guthrie
Ranking Member
Subcommittee on Oversight
and Investigations

[1] *Pandemic Advances Cybersecurity Efforts at HHS as Agency Becomes Bigger Target*, CISO Says, Meritalk, (August 19, 2020).

[2] *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*, Bloomberg (March 16, 2020).

Attachment #6

October 7, 2020

Dear Chairmen Pallone and Doyle,

On behalf of the undersigned organizations representing health plans, providers and consumer advocates, we thank you for hosting the September 17th hearing on the Federal Communications Commission (FCC). Throughout the hearing, committee members raised questions in regard to the FCC's response to the coronavirus pandemic. Noticeably absent from the discussion was the FCC's role in regulating communications between healthcare entities, such as insurers and physicians, and their patients. These communications are severely restricted today despite consumer interest in receiving the information and the measurable impact such communications have. We urge the Committee to address and resolve the Telephone Consumer Privacy Act (TCPA) barriers restricting critical healthcare information.

On March 20 the FCC declared the COVID-19 pandemic an "emergency" under the TCPA thereby exempting some COVID-related calls and text messages placed to consumers by healthcare providers and government officials from the typical TCPA requirements. Three months later, on July 28, the FCC issued another public notice clarifying that the March exemption applied to calls and text messages regarding plasma donation made by or on behalf of health care entities.

As a result of both orders, the healthcare community has:

- Contacted millions of Americans to provide COVID education and resources
- Provided clarity and information on benefits, including telehealth and behavioral health
- Encouraged patients to return to care and receive preventative medicine, including the seasonal flu vaccine
- Contacted public health authorities to facilitate patient transfers from COVID hotspots like nursing facilities
- Contacted members to assess their food security and provide supportive services

We thank the FCC for their swift action during this national, public health emergency. By its actions, the FCC underscored the impact such communications can have generally, and specifically preventing and slowing the spread of the virus. However, the emergency orders are limited in scope and duration, eventually expiring as the need to conduct these types of healthcare outreaches remain.

COVID-specific communications will certainly exceed the duration of the public health emergency declaration. For example, the frequency and interval of a forthcoming COVID vaccine could be more than once necessitating ongoing patient communications to ensure high vaccination rates. Some recovering and recovered patients may experience long-term symptoms and conditions that exceed the emergency order duration and who could benefit from these interactions.

Moreover, the long-term consequences of forgone care and social distancing are becoming increasingly apparent and will persist after the public health emergency itself. The Centers for Medicare and Medicaid Services (CMS) recently released information highlighting the significant and concerning decline in critical primary and time-sensitive preventative services for children. According to the September 23rd analysis, vaccinations are down by 22%, childhood screenings have declined by 44% and dental health services by 69%. CMS warns that missing these services can have long-term impacts on children's health outcomes.

Attachment #6

Adults are also forgoing preventative and in some cases urgent care. Recent analyses have shown that hospital admissions for heart attacks have declined by as much as 50% and the diagnosis of breast, colorectal, lung, pancreatic, stomach and esophageal cancers have dropped by 46% during the COVID outbreak. Unfortunately, it's unlikely that fewer patients are inexplicably having heart attacks or getting cancer.

Such health consequences can be mitigated through communications in a format that meets patients where they are, often via a cell phone, and are generated from their trusted healthcare network. In spite of the TCPA barriers, when such outreach is conducted measurable improvements are realized. In fact, direct patient engagement via phone calls and texts can improve vaccination rates by up to 30%, increase hypertension medication adherence by 25%, and cancer screenings by 45%. However, these communications occur infrequently or reach few patients because of the TCPA.

Additionally, as noted by many committee members during the hearing the frequency of localized natural disasters have increased, and to date such crises have not received TCPA exemptions. Yet, healthcare communications during those times are just as critical as COVID related communications are now. For example, before a hurricane, it's imperative to ensure patients on life-sustaining medications have timely information on early and extended refill authorizations in the event of sheltering or evacuation.

Finally, beyond the COVID public health emergency and natural disasters, our country faces ongoing "public health crises", including heart disease which sadly kills more than 655,000 Americans annually, and diabetes and cancer afflicting 10% and 5% of our population respectively. Patients with these conditions can benefit from ongoing interaction related to their care, yet because of the TCPA, important communications about their care, such as medication adherence, preventative care, and chronic disease management are rarely communicated via cellphone.

Our organizations have repeatedly raised concerns directly with the FCC in regard to the TCPA and sought to harmonize the TCPA with HIPAA to no avail. Therefore, we respectfully urge the Committee to work with the FCC to create a meaningful healthcare exemption to enable the healthcare community to address the long-term implications of COVID-19, conduct crises communications during localized disasters and emergencies, and to improve outcomes, empower patients and reduce costs in otherwise "normal" times. Enabling the types of patient communications described above should not be dependent on a time-limited emergency TCPA order.

On behalf of our organizations, we thank you for your leadership always and especially during this crisis. We also appreciate your consideration of our comments and look forward to working with the Committee on this issue.

Sincerely,

Anthem

BlueCross BlueShield Association

HEALTHCARE LEADERSHIP COUNCIL

hms

cc: Members of the House Energy and Commerce Committee

Attachment #7

Diane Sacks LLC

September 2020

Privacy and Security Round Up

Senate Republicans Release Privacy Bill

On September 17, 2020, Senator Wicker (R-Miss.), Chairman of the Senate Committee on Commerce, Science and Transportation, joined by several other Republican Senators, introduced a privacy bill, the SAFE DATA Act. The bill builds on a staff draft released by Senator Wicker in November 2019, but also incorporates provisions from two other bills, namely, the Filter Bubble Transparency Act (that would require internet platform to notify users when they use "opaque algorithms" to vary displayed content using user-specific data), and the DETOUR Act (designed to protect consumers against deceptive online user interfaces). The privacy provisions of the bill follow the traditional notice and consent model for the collection and use of most personal data, although the bill does have a fairly broad list of exceptions for which consent is not required. The bill gives consumers access, correction, deletion and portability rights to their data, again subject to a fairly extensive list of exceptions. It requires covered entities to implement security practices and data minimization, and requires large data holders to perform privacy assessments. The bill would be enforced by the Federal Trade Commission (FTC) and state attorneys general. The bill would preempt state privacy laws except for data breach notification laws. Activities subject to certain federal laws, such as Gramm-Leach-Bliley and HIPAA, would not be subject to the bill.

Comments: The bill appears to lay down a marker by Republicans of their priorities for privacy legislation next year. While it follows previous Republican bills in not providing for a private right of action and preempting most state privacy laws, its failure to preempt state data breach notification laws and to cleanly exempt HIPAA entities is likely to be a disappointment to many in the business and health community.

California Governor Signs into Law Two Bills Affecting the California Consumer Privacy Act (CCPA)

On September 25, 2020, California Governor Newsom signed into law AB 713, which amends the CCPA by: (1) creating a new exemption for certain data de-identified in accordance with HIPAA as long as the data is not re-identified; (2) extending to business associates the exemption for patient data maintained, used or disclosed in the same manner as PHI subject to HIPAA and California Medical Information Act; (3) expanding the exemption for clinical trial data to include data used in any research (as defined in HIPAA), provided certain conditions are met. AB 713 also imposes new requirements on data de-identified in accordance with HIPAA, including limitations on re-identification, and notice and contracting requirements. The second bill, AB 1281, signed into law on September 29, 2020, extends the CCPA partial exemptions for business-to-business (B2B) and employee personal information to the end of 2022 in the event Proposition 24 (enacting the California Privacy Rights Act (CPRA)) is not approved by voters in the November ballot. If CPRA is enacted, it would extend these exemptions through 2023. Thus, irrespective of what happens with Proposition 24, the two partial exemptions are extended at least through 2022.

Comments: AB 713 is positive news for businesses subject to the CCPA. However, the "exemption" for data de-identified under HIPAA is less of an exemption than at first appears in that AB 713 impose various requirements with respect to this data. As such, it operates much like a stricter de-identification standard. Both bills make clear that privacy law in California is anything but settled, and that will be especially the case if CPRA becomes law.

OCR Continues Its HIPAA Right of Access Initiative

On September 15, 2020, the Department of Health and Human Services Office of Civil Rights (OCR) announced enforcement actions against five health care providers for violations of the HIPAA requirement to provide patients with access to their health records. In announcing the settlements, OCR Director Roger Severino stated that the settlements were "about empowering patients and holding health care providers accountable for failing to take their HIPAA obligations seriously enough." OCR noted that it considers a variety of factors in determining the amount of a settlement, including the nature and extent of the potential HIPAA violation; the nature and extent of the harm resulting from the potential HIPAA violation; the entity's history with respect to compliance with the HIPAA Rules; the financial condition and size of the entity, and the impact of the COVID-19 public health emergency.

Comments: While the settlement amounts were relatively small (between $3,500 and $70,000), the announcement is significant in signaling OCR's continued focus on enforcing a patient's right to receive copies of their medical records. OCR announced its "HIPAA Right to Access Initiative," in early 2019, stating that it would "vigorously enforce the rights of patients to get access to their medical records promptly, without being overcharged, and in the readily producible format of their choice."

OCR Announces Several Significant HIPAA Settlements

In quick succession on September 21, 23 and 25, 2020, OCR announced three HIPAA settlements exceeding $1 million. The first was with Athens Orthopedic Clinic, following a hacking incident that affected over 200,000 patients. OCR found "longstanding, systemic noncompliance" with the HIPAA Privacy and Security Rules, including failures to conduct a risk analysis, implement risk management and audit controls, HIPAA policies and procedures, business associate agreements, or provide HIPAA training. The second was with CHSPSC for $2.3 million, also relating to a hacking attack, this time affecting over six million individuals. In this case the FBI had notified CHSPSC of the threat but, despite this, the hackers were able to access and exfiltrate patient records for a period of 4 months. OCR again found similar "longstanding, systemic noncompliance" with the HIPAA Security Rule. The third settlement was with Premara Blue Cross (PBC) for $6.85 million, again involving a hacking attack, this time affecting 10.4 million individuals. In this case the hackers had access to PBC's IT system for nearly 9 months before being detected. OCR again found "systemic noncompliance" with the HIPAA Rules, including failure to conduct an enterprise-wide risk analysis, implement risk management, or audit controls.

Comments: While these settlements appear to be wrapping up investigations of events that occurred several years ago, their similarities and announcement within a matter of days of each other sends a clear message that OCR will deal severely with "systematic noncompliance" with HIPAA. This is particularly the case when the noncompliance results in a significant delay in detecting or acting upon unauthorized system access, since this causes far greater harm to individuals than would otherwise have occurred.

Court Dismisses Lawsuit against University of Chicago Medical Center and Google

On September 4, 2020, a United States District Court for the Northern District of Illinois dismissed a lawsuit filed by a patient against the University of Chicago Medical Center (UCMC) and Google in June 2019 in connection with their 2017 collaboration to use machine learning techniques to predict hospitalizations and identify instances where a patient's health is declining. The lawsuit claimed, among other things, that UCMC's disclosure of the patient's records to Google violated HIPAA and was therefore a breach of its agreement with the patient to comply with HIPAA. The judge concluded that even if there was a basis to claim such a breach of contract, the patient had failed to show that it had caused him economic damages.

Comments: The decision has been hailed as a victory for Google, which entered into similar arrangements with other medical centers, including one with Ascension, which drew considerable public scrutiny. However, despite this victory, it is notable that the court determined that UCMC had potentially breached its contract with the patient by engaging in a "sale" of PHI in violation of the terms of its Notice of Privacy Practice. This potential "sale" was the provision of PHI to Google for research purposes in exchange for a license to use the Google software, even though this transaction fell within a HIPAA exception to the sale of PHI.

Please contact Diane Sacks at dsacks@sacksllc.com or (202)459-2101 for more information on any of these items. This newsletter is intended to provide general information only and is not intended as legal advice.

Attachment #8

Spam calls are hindering efforts to contact trace and track Covid-19

By Faith Karimi, CNN

Updated 8:12 AM ET, Tue October 6, 2020

(CNN) Nine months into a pandemic that has killed 210,000 people in the United States, health officials are imploring residents to answer their phones. The caller may be a disease tracker trying to save you from the deadly coronavirus.

Contact tracing involves identifying sick people, isolating them and then tracing everyone with whom they've been in contact and putting those people into quarantine.

But many people wary of spam calls and phishing scams are not answering calls from unknown numbers, undermining efforts by contact tracers to reach people exposed to Covid-19. And some states such as Louisiana are sending letters to those people who don't answer -- not the most effective way when time is of the essence.

Without a federal contact tracing program, health departments have set up a patchwork of procedures. Some have worked with phone companies to ensure the name of the health department shows up on caller ID. For example, in Washington, DC, it shows up as DC Covid 19 Team.

Still, others appear as unknown numbers and are getting mistaken for spam calls. And even when they show up with the specific departments, some are still going unanswered.

"Hello? Yes, it's you we're looking for," Mayor Muriel Bowser tweeted, echoing the Lionel Richie song. "Contact tracing is a critical tool in getting our city back on its feet. Answer the call."

The governor of Ohio is voicing the same message. State health officials say while they have 113 health jurisdictions and don't collect the percentage of calls answered on a state level, local jurisdictions have reported less cooperation with tracers now than they did earlier in the pandemic.

"If you receive a call from a contact tracer -- answer the call," Gov. Mike DeWine said. "Contact tracing is incredibly important as we work to stop the spread of Covid 19."

Robocalls have made things more complicated

In the age of identity theft, many Americans are rightly suspicious about sharing their personal information with strangers. And robocalls have not made things easier.

Attachment #8

The number of robocalls received in the United States dipped in the early months of the pandemic, then ticked back up as call centers reopened.

In September alone, there were 3.8 billion robocalls recorded nationwide by tracking service YouMail. That's about 127 million per day and an average 12 calls per person. With the desperate wait for coronavirus treatments and vaccines, scammers preying on pandemic fears are using such calls to offer bogus testing or seek personal information.

That has made people even more reluctant to share personal details by phone. For example, 45% of New Jersey residents with coronavirus reached by contact tracers refused to provide information for various reasons.

"This is about public health. No one is on a witch hunt here. We don't condone underage drinking, illegal behavior, but that is not what this is about," Gov. Phil Murphy said in July after a cluster of coronavirus cases was traced to a teens' house party. "No one has any questions other than have to do with stopping the spread of the virus."

Washington, DC, health officials said they have added contact tracers who will visit homes when people don't complete interviews or are unreachable by phone. "If contact tracers do not hear back, a text message will be sent with a home visit time and date, and visits may be conducted without confirmation," the health officials said.

Even when people answer, responses are spotty

Contact tracing largely relies on the public to voluntarily provide information. But when people do answer their calls, they are not always forthcoming, even though their identity and information is confidential and won't be shared with their contacts.

In Louisiana, where incoming calls from contact tracers say LA Health Dept, health officials have reached 66% of residents who tested positive since May. Another key challenge is getting details from people with whom they've been in contact, said Sean Ellis, a spokesman for the Louisiana Department of Health. Others have been displaced after Hurricane Laura, adding another layer of challenge.

Georgia also is facing challenges in reaching out to potential patients, partly because calls to cell phones only show a number. On some landlines, the Caller ID displays GDPH -- Georgia Department of Public Health. About 60% of contact tracing calls are being answered in the state's northwest health district, said Logan Boss, a spokesman for the Georgia Department of Public Health.

In Boss' district, health officials are sending text messages beforehand and if they can't reach people, they follow up with a call. If they still don't get a response, they send an email asking someone to reach out to them.

Some people are not calling back while others are withholding information on close contacts or employers, Boss said.

Attachment #8

In Columbus Ohio, incoming calls just show a general number with the local area code.

"We find that some people are reluctant to answer questions because they think it's a scam or because they don't want to be identified as a case or a contact, or provide information about other contacts, so they won't have to quarantine for 14 days," said Kelli Newman, a spokeswoman at Columbus Public Health.

Ohio's Cuyahoga County is getting 90-95% of its calls from contact tracers answered, said Kevin Brennan, a spokesman for the board of health. The number on the caller ID shows as being from the Ohio Department of Health.

If people don't answer, they get a text message in addition to a voice mail that identifies the caller as from the board of health. If an attempt to call three times is not successful, a letter is hand-delivered.

"We are finding, as time goes on, that people are reluctant to give us their contacts. If people question where we are calling from, we direct them to our website so that they can verify our employment," Brennan said.

While there's no federal contact tracing framework or app, the Centers for Disease Control and Prevention provides guidance and support to help local governments. It's up to each state local governments to decide what works best, the CDC says.

There's no federal contact tracing program, even though coronavirus cases are rising again in many states. So local health departments, already strained during the pandemic, have stepped in to track and limit the spread of the virus.

Contact tracing and testing are crucial to squelching coronavirus until there's a widely distributed vaccine or therapeutic drug, said Steve Waters, founder of Contrace Public Health Corps, which provides guidance on Covid-19 contact tracing.

Apple and Google systems can send you notifications about exposure to people with Covid-19.

"Contact tracing can still be effective without a 100% contact rate, however 100% is the goal, and the more the public participates, the more effective contact tracing will be," he said.

The more successful programs are reaching 80% to 90% of the people they contact -- and the faster they reach them, the better. At Waters' organization, most of the tracing is done over the phone. But if his callers reach someone who is uncomfortable discussing their information on the phone, personal visits can be arranged.

Successful programs have strong messaging in the hardest-hit areas to increase awareness about contact tracing so people will answer their phones, Waters said.

"Until the arrival of a widely available therapeutic or vaccine, testing and contact tracing are the best tools we have to fight the spread of Covid-19," Waters said. "I know there's a lot of fatigue

Attachment #8

right now with Covid measures but contact tracing is an important targeted way that the public can use to help protect people in their communities and the people closest to them."

In Columbus, health officials are running a multimedia contact tracing campaign to educate people about their efforts, Newman said.

To gain the upper hand against an unrelenting virus, health officials will need all the help from the public they can get.

Attachment #9

Pharmaceutical & Life Sciences News

The Virus Shot Goes in Your Arm, but Where Does Your Data Go?

By Jacquie Lee

Sept. 23, 2020, 5:59 AM

- Federal law may not cover personal data at all times
- Varying state laws leave consumers without consistent privacy protections

Patching together state immunization databases with information held by pharmacies like CVS, Walmart, and Walgreens to track Covid-19 vaccinations opens the door for misusing patient data, lawyers warn.

The Department of Defense is working with states and private companies to allow immunization databases to share data as part of a vaccine distribution plan. The system will allow someone who gets a shot at their local health center in one state to walk into a local pharmacy in a different state and figure out when they need their next dose and which vaccine they should take, according to Department of Defense official Paul Ostrowski, who's in charge of supply and distribution for a Covid-19 vaccine.

Keeping tabs on which vaccine someone took will help health providers remind people to get their second dose if it's necessary and make sure they're getting the right vaccine. However, neither the Department of Health and Human Services nor the Department of Defense has released details about the contracts outlining privacy obligations or how the private companies can use the data.

The Centers for Disease Control and Prevention released more details this week about how the government plans to track side effects of a shot in first responders, who are expected to be the first inoculated. That includes sending daily texts asking about side effects, which will have an opt-out option.

That raises red flags, lawyers and policy consultants say, because without a clear outline of how the data will be protected, companies could use immunization data for commercial purposes and consumers might not be protected equally if there is a data breach.

Patchwork Protections

"Although a very large number of states have strengthened their state breach notification laws and that sort of thing, there really is still a patchwork system in place," Linda Malek, chair of Moses & Singer's health-care and privacy practices, said.

States could differ on what data points are protected and when organizations have to disclose there's

Attachment #9

been a breach, she said. Certain states, like Texas, have rules around using personal data for marketing, but other states don't have those sorts of protections for consumers, she said.

Certain health data is protected under the Health Insurance Portability and Accountability Act. Depending on how the vaccine data contracts are worded, the law might not apply to every party utilizing the databases in every instance.

Consequently, if the federal health privacy law doesn't cover all the data at all times and the contracts don't include stipulations about how companies can use the data, there's "absolutely" instances where some consumers' privacy will be better protected than others, Malek said.

Walgreens will "continue to collaborate with the Administration, CDC and HHS on Covid-19 testing and vaccines," spokesperson Kelli Teno said. She didn't share additional details. CVS and Walmart didn't respond to questions about patient privacy and how they'll use the combined data.

What Happens After a Breach?

If something were to go wrong—like a data breach—whether the information is protected by the federal health law "really depends on how they set up the system and where the incident occurred," Dianne Bourque, a health privacy lawyer at Mintz in Boston, said. A health-care provider such as a doctor or pharmacist could enter vaccine information into the database system, she said, but if a breach occurred when the data was in the state government's hands, the responsibility falls on the government.

"Once it's out of the hands of the health-care provider, it's outside HIPAA," she said.

The law extends to the "business associates" of health-care providers too, but it isn't clear how that arrangement will work under this coronavirus vaccine system.

"It depends on whether there is a contractual arrangement between pharmacies and states and what each entity's role is," Malek said. "So how you structure the business arrangement could drive the legal regulatory ramifications of it."

If data isn't covered by HIPAA, it's less clear how a breach would be handled and who will be notified.

The opaque nature of contracts between the government and private companies to respond to the coronavirus pandemic has been a concern for government watchdogs since the pandemic began. Ostrowski told reporters last week those database contracts would be "releasable to an extent" at "some point in time" but that "not everything will be released."

Targeted Marketing

A silver lining of including private companies is their desire to protect their reputations, Bourque said. That means health-care providers will be "extraordinarily careful."

But for former government officials like Lisa Bari, leaning so heavily on private companies during a

Attachment #9

pandemic is concerning. Bari worked on health IT and data sharing within the Centers for Medicare & Medicaid Services before creating her own health IT consulting firm, Emphasis Health.

"We have a very fragmented health-care system with for-profit entities that serve a public health function that otherwise would be taken care of by the state in other countries," she said.

One of Bari's biggest concerns is companies using data for commercial purposes.

"You can create a behavior profile for anything," she said, referring to a marketing tactic used to tailor advertisements to specific people based on what a company knows about them.

"They may say they would not do it and that's fine, but for-profit health care enterprises making volunteer attestations that they won't violate privacy is not as good as not creating that situation in the first place," Bari said. "Better to not give someone that temptation even if they're not intending to harm someone's privacy."

To contact the reporter on this story: Jacquie Lee in Washington at jlee1@bloomberglaw.com

To contact the editors responsible for this story: Fawn Johnson at fjohnson@bloomberglaw.com; Andrew Childers at achilders@bloomberglaw.com

Attachment #10

Apple has the potential to make big waves in health care

Dain Evans

Apple has made some bold moves into health care, a market worth trillions globally. Most recently, it announced a blood oxygen sensor on the Apple Watch Series 6 and a partnership with the Singaporean government to incentivize Apple Watch users to be more healthy. But the company's strategy is a bit elusive as it walks the fine line between wellness and medicine.

Apple has three areas of focus when it comes to health: hardware, like the Apple Watch, software, like the Health App and ResearchKit, and services, like Fitness+, Apple's newest subscription service.

Most of these devices and services revolve around the iPhone ecosystem. While iPhone sales are still the majority of Apple's revenue, wearables and services are quickly picking up steam. iPhone sales have increased an average of about 4% quarter-over-quarter, and about 2% year-over-year since 2017. Services have increased an average of about 4.5% quarter-over-quarter, and about 22% year-over-year since 2017. Apple doesn't break out revenue for the Apple Watch but its "wearables, home and accessories" business, which includes AirPods, Apple Watch and other accessories, has grown the most by far, increasing at an average of almost 9% quarter over quarter, and nearly 35% year-over-year since 2017. The segment earned $6.45 billion in revenue during the third quarter of 2020.

With these products and services creeping closer and closer to medicine and medical devices, Apple has had to meet new regulations from the Food and Drug Administration. The FDA oversees the clearance and approval of medical devices for safety and standards.

Apple has found creative ways to get FDA approval without declaring itself as a medical device manufacturer. The Apple Watch has a De Novo classification under the FDA for its ECG feature, meaning it is the first of its kind, and therefore cannot be compared to anything else on the market regarding standards. Apple may continue to add new health-monitoring features. It has discussed adding a blood glucose monitor, for example.

And Apple has made some big deals with health-care institutions, health records companies, and even governments. The company announced it would partner with the Singaporean government to give resident Apple Watch users up to $380 Singapore dollars if they engage in healthy behaviors like exercise or meditation.

It has also entered a new battleground through health initiatives, in some cases, is already participating in the same markets as Peloton, Abbott and medical record software-maker Epic.

Attachment #11

Bigger health systems aren't doing a better job at cybersecurity, report finds. Here's why

by Heather Landi
Sep 18, 2020 3:15pm

Only 44% of healthcare organizations, including hospitals, health systems and third-party vendors, are meeting national cybersecurity standards designed to protect against cyberattacks.

And bigger healthcare institutions with larger budgets didn't necessarily perform better when it comes to security, according to a new report from cybersecurity firm CynergisTek. In fact, big organizations sometimes performed worse than smaller organizations or those that invested less, the report found.

In some cases, this was a direct result of consolidation where systems directly connect to newly acquired hospitals without first shoring up their security posture and conducting a compromise assessment, according to CynergisTek.

Analysts at the Austin, Texas-based security firm examined nearly 300 assessments of provider facilities, including hospitals, physician practices, accountable care organizations and business associates, to determine how well they are conforming to the National Institute of Standards and Technology’s Cybersecurity Framework (NIST CSF) protocols, which are considered security best practices.

Looking at historical client data, CynergisTek found cybersecurity scores in some cases trending backward since 2017.

In 2017, CynergisTek's assessment found 45% of organizations complied with NIST cybersecurity protocols. There was a measurable uptick to 47% in 2018. In 2019, a year with a record number of attacks and breaches in healthcare, that average had dropped to 44%.

In 2019, 79% of facilities scored less than a C in terms of conformance with the NIST cybersecurity best practices, the report found.

Leading factors influencing performance include poor security planning and lack of organizational focus, inadequate reporting structures and funding, confusion around priorities, lack of staff and no clear plan, the report found.

This decline in overall conformance should be an alarming call to action for the industry, not just for IT and security leaders, CynergisTek said.

Attachment #11

While healthcare’s focus on information security has increased over the last 15 years, investment is still lagging, according to David Finn, executive vice president of strategic innovation at CynergisTek.

"In the age of remote working and an attack surface that has exponentially grown, simply maintaining a security status quo won’t cut it," he said. "The good news is that issues emerging in our assessments are largely addressable. The bad news is that it is going to require investment in an industry still struggling with financial losses from COVID-19.”

The healthcare industry also is looking down the barrel at new regulations that will complicate cybersecurity.

Interoperability and information blocking rules, which go into effect in just a few months, mean even more data sharing with more people, places and devices. The overall decline in conformance—as the healthcare industry enters a post-COVID-19 world, and issues around privacy and new interoperability and information blocking rules become effective—does not bode well for where the sector needs to be, according to the report.

The report also found that healthcare supply chain security is one of the lowest ranked areas for NIST cybersecurity protocol conformance. This is a critical weakness, given that COVID-19 demonstrated just how broken the healthcare supply chain really is with providers buying personal protective equipment (PPE) from unvetted suppliers, CynergisTek said.

"The problem is [healthcare organizations] are not investing fast enough relative to an innovative and well-resourced adversary,” said Caleb Barlow, president and CEO of CynergisTek, in a statement.

There are some bright spots, however. "Organizations that have invested in their programs and had regular risk assessments, devised a plan, addressed prioritized issues stemming from the assessments and leveraged proven strategies like hiring the right staff and evidence-based tools have seen significant improvements to their NIST CSF conformance scores," Barlow said.

CynergisTek offered some key strategies for healthcare organizations to bolster their security defenses.

- **Look under the hood at security and privacy amid mergers and acquisitions:** For health systems planning to integrate new organizations into the fold through mergers and acquisitions, leadership needs to be more diligent when examining the organization’s security and privacy infrastructure, measures and performance. It’s important to understand their books and revenue streams as well as their potential security risks and gaps to prevent these issues from becoming liabilities.
- **Make security an enterprise priority:** Understanding how these risks tie to the bigger picture will help an organization that thinks it cannot afford to invest in privacy and information security risk management activities understand why making such an investment is crucial. Hospitals and healthcare organizations should create collaborative,

Attachment #11

cross-functional task forces like enterprise response teams, which offer other business units an eye-opening look into how security and privacy touch all parts of the business.

- **Money isn't a solution:** Security leaders need to identify priorities and have a plan that leverages talent, tried-and-true strategies like multifactor authentication, privileged access management and ongoing staff training to truly level up their defenses and take a more holistic approach.
- **Accelerate the move to the cloud:** While healthcare has traditionally been slow to adopt the cloud, these solutions provide the agility and scalability that can help leaders cope with situations like COVID-19 and other crises more effectively.
- **Shore up security posture:** COVID-19 taught us that workflow can also disrupt security, and things are going to get worse before getting better. Get an assessment quickly to determine immediate needs, and come up with a game plan to bolster defenses needed in this next normal.