Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

COVID-19: Digital Contact Tracing and Privacy Law

July 9, 2020

Many states, territories, and localities have implemented public health orders to limit the spread of Coronavirus Disease 2019 (COVID-19) in their respective communities, including stay-at-home orders, orders temporarily closing schools and businesses, and orders limiting the size of public gatherings. In preparation for the eventual relaxation and lifting of these orders, the Centers for Disease Control and Prevention (CDC) have advocated that public health authorities use robust "contact tracing" procedures to prevent the reoccurrence of widespread infections after communities reopen. While federal entities may advise on these procedures, state and local authorities are responsible for contact tracing operations, as provided by state law.

The term "contact tracing" generally refers to identifying and monitoring people who have been in contact with someone diagnosed with an infectious disease, in order to locate other potentially infected individuals quickly and take targeted control measures (such as quarantines) to prevent the broader spread of the illness. Contact tracing is standard procedure in public health investigations, and historically involves officials interviewing and contacting infected and potentially-exposed persons. However, some of the contact tracing proposals aimed at controlling the spread of COVID-19 suggest supplementing traditional contact tracing procedures with technology to collect data electronically. These proposals raise questions about how federal laws governing health information privacy may apply to electronic or digital contact tracing. One such provision is the "HIPAA Privacy Rule," which refers collectively to regulations promulgated by the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA). This Sidebar discusses the HIPAA Privacy Rule's application to digital contact tracing and briefly discusses other federal laws that regulate data privacy.

HIPAA Privacy Rule Overview

The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI) by "covered entities" and their "business associates." Covered entities include health plans, health care clearinghouses, and "health care providers" who transmit electronic health information in connection with a HIPAA-covered transaction (such as billing). A health plan is an "individual or group plan that provides, or pays the cost of, medical care." This includes health insurance companies, health maintenance organizations (HMOs), and government programs, such as Medicaid and Medicare, that pay for

Congressional Research Service
https://crsreports.congress.gov
LSB10511

healthcare. Health care clearinghouses are defined as entities that process health information in a nonstandard format into a standard format, or vice versa. Lastly, health care providers include providers of services covered by Sections 1861(u) or 1861(s) of the Social Security Act (which includes, among other things, physicians' services, hospital services, physical therapy services, and skilled nursing facility services) or any person who otherwise "furnishes, bills, or is paid for health care in the normal course of business." Health care is defined as "care, services, or supplies related to the health of an individual." A business associate is one who, among other actions, "creates, receives, maintains, or transmits protected health information" on behalf of a covered entity for an activity regulated under HIPAA generally (not simply the Privacy Rule), such as claims processing, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing.

The HIPAA Privacy Rule recognizes that entities may engage in conduct that makes them covered entities ("covered functions"), while, at the same time, performing other functions that would not render them covered entities. For instance, institutions of higher learning may, in addition to providing education, run a health clinic that provides healthcare for students. Such an entity may become a "hybrid entity" by complying with organizational requirements that include designating a specific component of its organization as the "health care component." In such situations, only the designated health care component of a hybrid entity is required to comply with the HIPAA Privacy Rule.

As noted, the obligations of covered entities and their business associates under the HIPAA Privacy Rule revolve around the use and disclosure PHI. PHI includes information that (1) "identifies," or can reasonably "be used to identify," an individual; (2) is "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (3) relates to an individual's past, present, or future physical or mental health, health care provision, or payment for the provision of health care; and (4) is transmitted by or maintained in electronic or any other form or medium. The HIPAA Privacy Rule, among other things, limits covered entities from using PHI or sharing it with third parties without valid patient authorization, unless the use is for purposes of treatment, payment, or "health care operations," or falls within a specific statutory exception.

One such exception that is particularly relevant to contact tracing allows covered entities to use or disclose PHI—without individual patient authorization or the opportunity for the patient to agree or object—to "a public health authority" that is legally authorized to collect the information "for the purpose of preventing or controlling disease, injury, or disability," including "the conduct of public health surveillance." A "public health authority" includes any agency or authority of the "United States, a State, a territory, a political subdivision of a State or territory, or Indian tribe," that is "responsible for public health matters as part of its official mandate," as well as "a person or entity acting under a grant of authority from or contract with" such an agency. This definition encompasses the CDC as well as state and local public health departments, among others. State and local health departments may engage in both covered and non-covered activities, and many choose to designate themselves as a "hybrid entity," so that their non-covered components need not comply with the HIPAA Privacy Rule's requirements.

Violations of the HIPAA Privacy Rule can lead to civil or criminal enforcement. The HHS Office of Civil Rights is responsible for investigating and enforcing civil violations of HIPAA's requirements and may impose monetary penalties, which vary depending on the violator's culpability. The U.S. Department of Justice has criminal enforcement authority under HIPAA and may seek fines or imprisonment against a person who "knowingly" obtains or discloses "individually identifiable health information" or "uses or causes to be used a unique health identifier" in violation of HIPAA's requirements.

Mobile Application Contact Tracing Overview

Among the many challenges public health authorities face in tracking and controlling the spread of COVID-19 is that the disease is highly infectious and appears to be transmissible by people who do not

show symptoms of COVID-19 and thus may not know that they are infected. In this environment, mobile applications (apps) may facilitate public health authorities' gathering data on potential exposures to use in contract tracing. As explained in this CRS In Focus, governments and technology companies have explored two schemes for gathering device data through contact tracing apps: location tracking and proximity tracking. *Location tracking* schemes collect location information from individuals' mobile devices, including global positioning system (GPS) and cell site location information, to map their locations over time. *Proximity tracking* schemes use Bluetooth technology to determine when two devices remain within a particular distance of each other for a specified amount of time, without collecting location data. Apps built using either scheme relate information to a unique identifier associated with a particular mobile device. For location tracking apps, these identifiers are mapped to particular locations, while proximity tracking apps broadcast identifiers over Bluetooth so app users may anonymously log encounters with other app users. In certain app configurations, an app user may report a positive COVID-19 diagnosis within the app, which then could relay a report of that diagnosis—anonymously—to those app users who had been in proximity to the diagnosed person, and/or to public health authorities undertaking contact tracing investigations.

North Dakota and South Dakota have both deployed a location tracking system, while Google and Apple have changed their mobile operating systems to allow developers to create proximity tracking apps. Some apps may use both location and proximity tracking, such as an app previously deployed by Norway's government. In each case, app functionality may rely on several types of information with different sources, including information from the app user's device (such as the device's unique identifier) and information the app user voluntarily provides (such as a positive COVID-19 diagnosis).

Interaction of the HIPAA Privacy Rule with Mobile Application Contact Tracing

As noted, the HIPAA Privacy Rule's protections do not apply to all health-related data. Only PHI held by covered entities and their business associates is subject to the Rule. Thus, the extent to which the Rule applies to digital contact tracing applications depends on whether the parties developing the apps and processing app information fall within the definitions of covered entities or business associates and whether the app uses PHI.

Are public health authorities or app developers Covered Entities or Business Associates?

Because state and local public health authorities are the primary users of data collected through contact tracing, a critical threshold issue is whether they are *covered entities* subject to the HIPAA Privacy Rule. This issue is complicated by the fact that a public health authority may perform various functions within one agency. For example, a public health authority may provide clinical care (e.g., diagnostic testing), and thus qualify as a health care provider subject to HIPAA's requirements. The same agency might also engage in community-wide or state-wide disease control activities, such as contact tracing, that do not appear to be among the functions by which HIPAA defines covered entities.

Thus, a health department that engages in both health care activities and disease control functions may choose to operate as a "hybrid entity." In so doing, state and local health departments may limit their obligations under the HIPAA Privacy Rule solely to their performance of discrete covered healthcare functions. Any information the "hybrid" agency obtains for use in disease control activities such as contact tracing would not be subject to HIPAA's privacy protections. Moreover, under the public health authority exception to the HIPAA Privacy Rule, this would include PHI received by the public health authority from a covered entity, such as a healthcare provider.

Third-party software developers standing alone are not generally covered entities subject to the HIPAA Privacy Rule. Moreover, a third-party software developer that creates, maintains, or administers an app used in a public health authority's contact tracing operations would not qualify as a business associate subject to the HIPAA Privacy Rule if the public health authority is not a covered entity when performing its disease control functions. That is because, as explained above, HIPAA defines a business associate as one who "creates, receives, maintains, or transmits protected health information" on behalf of a covered entity.

Do contact tracing apps use PHI?

Even if an entity is a covered entity or a business associate under HIPPA, HIPAA's Privacy Rule only applies to PHI. To be sure, contact tracing apps rely on health-related information (e.g., information that shows whether individuals have been diagnosed with, or exposed to, COVID-19). Thus, for any entities involved in the development and operation of a contact tracing app that might be covered entities or business associates, the applicability of the HIPAA Privacy Rule to them would largely depend on whether the information used for digital contact tracing is *individually identifiable*.

HIPAA deems health information not identifiable if the covered entity takes either of two steps. One option is that the covered entity can de-identify the information by ensuring that eighteen specific types of identifiers have been removed (including, for example, "all geographic subdivisions smaller than a State," "telephone numbers," and "device identifiers"). Alternatively, the covered entity may obtain documentation showing that an expert has determined that there is a "very small" risk of identification from the information. If this approach is chosen, the HHS Office of Civil Rights may assess the expert's qualifications in the course of an audit or investigation.

It is difficult to conceive how covered entities could de-identify the information required for contract tracing apps to function. Contact tracing apps will necessarily depend on information that accurately tracks individual movements and contacts. Both location tracking and proximity tracking apps function by associating a person who has tested positive for a disease with a device identifier generated by the app. In the case of location tracking apps, this includes GPS or cell site location information, which provides geographic information much smaller than a state. Apps also could request additional identifying information: Singapore's app, for example, requires app users to provide phone numbers. Accordingly, the most likely option by which a covered entity could establish that the health information used for digital contact tracing is not identifiable would be to obtain an expert determination that the risk of identification from the information is "very small."

Any such determination would likely assess the steps taken by the app to make identification more difficult. Google and Apple's proximity tracking framework provides for apps that use randomly generated identifiers, which cycle every 10-20 minutes to reduce the risk of linking any group of identifiers to an individual. Location tracking apps may take similar measures to mitigate tracking risk. For example, North Dakota's app associates location information with a random ID number and only stores location information when a device remains at a location for more than ten minutes. However, even apps that associate information with randomly generated identifiers may be susceptible to "linkage attacks" in which an entity might be able to identify a particular device, and apps that collect more detailed information may pose even greater risks.

Other Relevant Privacy Laws

Even when HIPAA does not apply, other federal privacy laws may come into play. As discussed in this CRS report, HIPAA is just one part of the "patchwork" of federal laws governing companies' privacy obligations. In particular, the companies that develop and maintain contact tracing apps must comply with the Federal Trade Commission Act's prohibition on unfair or deceptive acts or practices (UDAPs). The

Federal Trade Commission (FTC), which enforces this prohibition, regularly brings enforcement actions against persons or companies for collecting or using personal information in a deceptive or unfair manner, such as when a company's privacy practices contradict its posted privacy policy. It is unclear, however, whether the FTC could bring a UDAP action against state health departments or app developers acting on their behalf. For example, courts have applied the state action doctrine—which provides immunity for certain state actions that might otherwise violate federal antitrust laws—to FTC suits brought under the FTC Act's prohibition of "unfair methods of competition." This doctrine may also apply to the FTC's UDAP authority. At least one district court has applied the state action doctrine to bar the FTC from using its UDAP enforcement power against a state entity, although that decision was later vacated on other grounds. However, the case law on this issue is relatively sparse.

Along with the FTC Act, the Communications Act may limit tracing apps' ability to gather cellphone GPS data. The Communications Act prohibits telephone carriers from using or disclosing "customer proprietary network information" (CPNI) unless the customer consents or a specific exception applies. The Act defines CPNI to include information relating to the "location" of a customer's "telecommunications service" that is available to the carrier by "virtue of the carrier-customer relationship." However, CPNI excludes "aggregate" customer information from which "individual customer identities and characteristics have been removed," similar to how companies like Google and Apple claim they are endeavoring to de-identify information with their contact tracing frameworks.

Considerations for Congress

In summary, no single federal law creates consistent, clearly-applicable privacy protections for the information that likely would be gathered and used in contact tracing activities. In the context of digital contact tracing, state and local health departments conducting contact tracing and the app developers that assist them in that activity may not qualify as covered entities or business associates subject to HIPAA's requirements. Other federal laws, such as the FTC Act and Communications Act, may provide some privacy protections when HIPAA does not apply. Yet the reach of these laws is also limited. The FTC does not require entities to adopt particular privacy practices; it only takes enforcement action against corporate and private actors that it believes are engaged in unfair or deceptive conduct. The Communications Act's CPNI protections apply only to telephone carriers.

Members of the 116th Congress have proposed several COVID-19-related privacy bills. While an in-depth discussion of these bills is beyond the scope of this Sidebar, the Public Health Emergency Privacy Act (PHEPA), COVID–19 Consumer Data Protection Act of 2020 (CCDPA), and Exposure Notification Privacy Act (EPNA) would generally provide additional privacy rights and obligations related to entities' collection and use of personal information for contract tracing and exposure notification purposes. While the CCDPA and PHEPA would apply specifically to COVID-19, the EPNA would not be limited to the current pandemic. For a further discussion of these bills, see CRS Legal Sidebar LSB10501, *"Tracing Papers": A Comparison of COVID-19 Data Privacy Bills*, by Jonathan M. Gaffney. For a discussion of Congress's constitutional authority to regulate states' contact tracing activities, see CRS Legal Sidebar LSB10502, *Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data*, by Edward C. Liu.

Author Information

Eric N. Holmes
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Disclaimer