As the coronavirus spreads across the globe and in the United States, providers, businesses, employers, and others are struggling to understand what medical information they can collect and what information they can share. These are difficult questions the answers to which involve considering factors such as long-standing compliance requirements (e.g., HIPAA, ADA, GINA, state law), the unprecedented times we are in, business risk, and common sense. Government is trying to act to relieve some of these challenges, but questions still remain.

**HIPAA Privacy Rule Waiver of Penalties and Sanctions**

Effective March 15, 2020, for example, Secretary of the U.S. Department of Health and Human Services (HHS) Alex M. Azar (Secretary) waived certain penalties and sanctions under the HIPAA Privacy Rule against hospitals in its March 2020 COVID-19 and HIPAA Bulletin. These waivers were issued in response to President Donald J.
Trump’s declaration of a nationwide emergency concerning COVID-19, and the Secretary’s earlier declaration of a public health emergency on January 31, 2020. The Secretary’s guidance makes clear that the Privacy Rule is not suspended during this crisis and provides guidance about the ability of entities covered by the HIPAA regulations to share information, including with friends and family, public health officials, and emergency personnel. But, in the following areas, the Secretary has waived sanctions and penalties against covered hospitals that do not comply with the following provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient’s agreement to speak with family members or friends involved in the patient’s care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient’s right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient’s right to request confidential communications. See 45 CFR 164.522(b).

The waiver became effective on March 15, 2020, and there is more information and access to resources in the Bulletin about where it applies and for how long.

**Reminder About What Entities Are Covered Entities and Business Associates**

As part of its guidance on HIPAA privacy and disclosures in emergency situations, the Bulletin reminds readers what entities are covered by these rules – covered entities and business associates. There can be some tricky questions here, but these are the basic rules from the Bulletin:

*The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity’s or business associate’s workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information. Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.*
Employers are Not Covered Entities or Business Associates – But Still Have Privacy and Confidentiality Obligations

When conducting its business, an organization can be a HIPAA covered entity and/or a business associate. However, when that business is functioning as an employer, it is neither a HIPAA covered entity nor a business associate, although it may sponsor a covered health plan subject to the HIPAA privacy and security rules. As organizations face the coronavirus threat to their workforce and their business, many questions arise about the collection, processing, and disclosure of medical information from employees, their family members, and visitors to their facilities. These can be thorny questions and organizations should seek qualified counsel, but here are some general rules:

When may an ADA-covered employer take the body temperature of employees during the COVID-19 pandemic?

Generally, measuring an employee’s body temperature is a medical examination. This means that under the ADA, taking an employee’s temperature generally would be impermissible unless it was job-related and consistent with business necessity. However, because the CDC and state/local health authorities have acknowledged community spread of COVID-19 and issued attendant precautions, employers may measure employees’ body temperature. See additional questions at the EEOC’s What You Should Know About the ADA, the Rehabilitation Act, and COVID-19.

When an employer collects employee temperature functioning as an employer, such as in connection with protecting its workforce during the COVID-19 pandemic, is that information subject to the HIPAA Privacy Rule?

No. As stated above, employers acting as employers are not covered entities or business associates under HIPAA.

What about an employee’s family members, can an employer ask employees whether their family members have coronavirus?

In general, the ADA does apply here, although employers need to remember to avoid discrimination against a person because of his or her known relationship or association with a person with a known disability. The more relevant issue is whether the employer would be collecting “genetic information” under the Genetic Information Nondiscrimination Act (GINA), which includes the manifestation of disease in a family member. Genetic information under GINA including the manifestation of disease in a family member including a spouse, and the collection of that information generally is prohibited, except in limited circumstances.

What about state law? If EEOC guidance permits collecting employee temperatures during this pandemic, do employers have to consider state law?

Yes. For example, California’s Department of Industrial Relations’ Coronavirus Disease (COVID-19) – FAQs provide:
Can an employer require a worker to provide information about recent travel to countries considered to be high-risk for exposure to the coronavirus?

Yes. Employers can request that employees inform them if they are planning or have traveled to countries considered by the Centers for Disease Control and Prevention to be high-risk areas for exposure to the coronavirus. **However, employees have a right to medical privacy, so the employer cannot inquire into areas of medical privacy.** (emphasis added).

California also has other limitations on the collection of employee medical information, such as constitutional protections and limitations on the collection of personal information under the California Family Rights Act (“CFRA”). In California and other states, if this information is accessed and/or acquired by an unauthorized party, it could result in a breach of security, requiring notification. Many states also recognize common law privacy rights, such as protection from intrusion upon seclusion. While these common law rights generally would present a low risk, the circumstances of the collection could expose the organization to liability.

We heard about the California Consumer Privacy Act (CCPA), does that affect what we can collect?

Generally, no, the CCPA does not prohibit covered businesses from collecting personal information. If your organization is subject to the CCPA, you will want to consider whether an exception applies. For example, medical information under the California Confidentiality of Medical Information Act (CMIA) is excluded from the CCPA.

Section 56.05 of the CMIA defined medical information as

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment. “Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity. (emphasis added).

**Businesses subject to the CCPA** that collect medical information from California employees directly, without the involvement of health care professionals, may not be able to rely on the CMIA exception under CCPA. In that case, the businesses **notice at collection** should cover this information and describe the purpose(s) that information will be used. The same may be true for California businesses that, for example, are directing security personnel to collect temperature from non-employee visitors to their facilities.

**What about if we know an employee tested positive for COVID-19, can we share the employee’s identity with other employees so they can take steps**
to protect themselves and those around them, and prevent further spread?

According to the CDC,

*if an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the Americans with Disabilities Act (ADA). Employees exposed to a co-worker with confirmed COVID-19 should refer to CDC guidance for how to conduct a risk assessment of their potential exposure.*

EEOC’s ADA regulation 1630.14(d)(4)(i) says that any medical information regarding the medical condition of an employee shall be treated as a confidential medical record, except:

- Supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations;
- First aid and safety personnel may be informed, when appropriate, if the disability might require emergency treatment; and
- Government officials investigating compliance with this part shall be provided relevant information on request.

The EEOC also has interpreted the ADA to allow employers to disclose medical information to state workers’ compensation offices, state second injury funds, workers’ compensation insurance carriers, health care professionals when seeking advice in making reasonable accommodation determinations, and for insurance purposes.

Difficult circumstances can present themselves during these times and organizations will have to consider the circumstances on the ground, weighing multiple factors as they decide how to respond to these and similar questions. For instance, an organization may determine its compliance risk is outweighed by its reputational and moral risks to those in its community, and the needs of local public health authorities. For those organizations that proceed where there is unclear regulatory guidance, some key principles should guide them:

- proceed cautiously and engage as minimally necessary,
- make clear the purpose and use and disclose information only as necessary to serve that purpose,
- ensure security is maintained for information, and destroy it when no longer needed, and
- remain aware of changes to federal and state guidance, particularly in localized areas.

These are no doubt challenging times. Organizations need to do the best they can weighing various factors including privacy rights, compliance, the health of others, the community, and legitimate business, just to name a few.