



Sep 08, 2021

Categories:

[Blogs](#)

[Coronavirus Response](#)

[Team](#)

[Health Law Matters](#)

[Publications](#)

Authors:

[Catherine F. Burgett](#)

[Fred Gaona III](#)

[Darren S. Skyles](#)

Maintaining Employee Medical Information and COVID-19

In employers' urgency to ensure proper procedures are in place to create a safe and healthy workplace to protect against the spread of COVID-19, employers must maintain the privacy and security of employee medical information. Whether creating a mandatory vaccination or testing policy, implementing contact tracing procedures or merely questioning individual employees about health status, employers may be collecting or creating medical information and documentation on their employees that must be properly maintained and only communicated as strictly necessary.

Navigating federal and state laws pertaining to protecting employees' medical information is essential. The Equal Employment Opportunity Commission (EEOC) emphasizes that while protection of medical information must be maintained during the pandemic, this should not interfere with employers doing what is necessary to follow Center for Disease Control and Prevention (CDC) guidance as well as that from state and local health authorities.

"COVID-19 and the Workplace: Legal Requirements Employers Should Know."

This article is part two of our four-part series.

Part 1: [Thinking About Implementing a Mandatory COVID 19 Vaccine Policy? Here Is What to Consider](#)

Part 2: [Maintaining Employee Medical Information and COVID-19](#)

Part 3: [Nursing Homes: Spread of COVID and Vaccine Mandates](#)

Part 4: Coming Soon

EEOC Requirements

The Americans with Disabilities Act (ADA) applies to employers with 15 or more employees. Medical information pertaining to an employee must be maintained separately and securely from the employee's personnel file. Only authorized personnel trained on maintaining the privacy and security of these files should have access. Medical information may include vaccine cards, employee

health screening information or the notes maintained from discussing an employee's health condition. Whether the medical information the employer retains is created through the employer (e.g., employee clinic) or by an outside party such as a doctor's office makes no difference; the information must be maintained separately and securely.

In addition to keeping such medical information locked away in storage files and secured electronically, employers should implement and routinely enforce policies and procedures to ensure there is no inadvertent disclosure of an employee's medical information. These include policies on maintaining private and secure workspaces (e.g., no stray notepads or public-facing computer screens to reveal medical information) and password-protection procedures for storing medical information electronically. Training the workforce on how to maintain the privacy and security of employee medical information is also advised and, in some employment settings, required.

State Law and other Federal Law Requirements

Most states have privacy and security laws pertaining to maintaining health information. Employers need to be aware of their state's (or states') laws pertaining to the allowable use and disclosure of health information, required security procedures, breach notification requirements and mandatory training of the workforce. Often, such states' privacy and security laws are stricter than what federal laws require, so merely following the ADA requirements may not be sufficient to ensure an employer is fully compliant with all applicable laws.

While many employers don't fall directly under the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules that pertain to a "Covered Entity"—defined as health plans, health care clearinghouses and health care providers—what an employer offers its employees may lead to the employer handling protected health information (PHI). Employers that provide a self-insured employee health plan, sponsor a group health plan or manage medical information

between employees and their health care providers or health plan should consult legal counsel to determine if there are any specific requirements pertaining to HIPAA, if they access and maintain PHI through one of these activities.

Disclosures of Medical Information

Maintaining a healthy work environment in the face of COVID-19 may require employers to communicate discreetly about an employee's medical information, but such disclosures must be held to a minimum and communicated strictly to the extent necessary. If an employer knows, for example, that an employee has COVID, the employer may communicate about an employee's diagnosis to take actions in line with CDC recommendations. The employee's identity should be provided only as required and only to those who have a specific purpose for knowing it (e.g., contact tracing purposes).

For any health incident, employers should have a list of specially trained individuals (e.g., those in human resources) who can confidentially assist with necessary health-related procedures addressing potentially infected employees. However, the employer must work to protect the infected employee's identity (or those infected) to the degree practicable. For example, the employer may communicate to a particular group that an unnamed person infected with COVID was in their workspace and give instructions on self-monitoring for symptoms. While this information may lead employees to conclude who was infected, the EEOC allows generic descriptions for advising on an employee's diagnosis that could affect the health of coworkers.

An employer might have to disclose the identity of the infected employee to other employees who need to quarantine due to high-risk exposure (e.g., anyone who was within 6 feet for more than 15 minutes). Employers should remind employees that all medical information is private and secure, and there will be disciplinary consequences for violating that privacy. Employers may also provide an employee's medical information to a public health agency as required by law (e.g., OSHA investigation, workers' comp claims, public health authorities, etc.) or may disclose an employee's COVID diagnosis to another employer, for instance, if

the employee was in the other employer's work site and exposed others.

The strictest protocols on confidentiality must be followed in terms of who is informed and the information disclosed. Any potential disclosure of an employee's medical information to others should be addressed with legal counsel prior to disclosing.

Conclusion

While employers are faced with many challenges, the proper maintenance and security of medical information should be a top priority. With closely followed clear and informed policies, employers should be able to navigate the federal and state law requirements pertaining to securing employee medical information.

For more information, contact [Darren Skyles](#), [Fred Gaona](#), [Cat Burgett](#), or any attorney with Frost Brown Todd's [Health Care Innovation](#) industry team and [Labor & Employment](#) practice group.

We've tagged this article as featured content because it was trending at the time of publication and drew considerable interest among our readers. Check out the latest trending articles and resource collections by visiting our [featured section](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.