Employees Mandated to Provide Proof of Vaccination – Now What?

October 28, 2021

By: Kerri Wright

Employment Law Monthly - October 2021

Both the federal government and a growing number of state governments have mandated vaccination and testing for employees. These mandates have left employers with the task of developing protocols for the collection, verification and storage of employees' proof of vaccination documentation. Employers must ensure that they are in compliance with U.S. Equal Employment Opportunity Commission ("EEOC") guidelines, which require that vaccination cards or any other confirmation of vaccination be treated as confidential. They also need to develop protocols for verifying those vaccination records and, in certain circumstances, considering disciplinary action in the event the verification process reveals that the employee presented a fraudulent vaccination record.

Confidentiality and Vaccination Cards

The EEOC has established that employers may request proof of vaccination from employees. In its latest guidance, released May 28, 2021, the EEOC addresses several topics including how employers should handle employees' vaccination records. Employers must limit access to vaccination records, like all medical information, by maintaining them confidentially in a file separate from an employee's regular personnel file. Medical information related to COVID-19 may also be stored in employee's existing medical file. According to the EEOC, an employee's statement that he/she has the disease, the employer's notes, or other documentation for questioning the employee about symptoms, and logs of daily temperature check results should be stored in the medical file.

Since a vaccination card is considered a medical record, it triggers retention obligations. Therefore, employers may consider having the employees present their card rather than submit it for collection. The employee would simply present the card or digital vaccination record to a manager who would then record the employee's vaccination status.

The EEOC guidance also explains that the employer must takes steps to ensure that employees' medical information is kept confidential even while working remotely. If a supervisor receives medical information regarding COVID-19 electronically, the supervisor must safeguard that information. Laptops and other devices are not to be left where others can access the protected information.

Some employers may be reluctant to share vaccination records that they have collected with other entities. The EEOC does not provide specific guidance about whether the vaccination record itself may be shared but does allow, for example, a staffing agency to share an employee's disease status with an employer. Since disease status is considered confidential information, and allowed to be disclosed, by extension it may be permissible to disclose vaccination information in this scenario. However, employers must ensure that they are not in violation of the Health Insurance Portability and Accounting Act ("HIPAA"). HIPAA is a federal law created to protect sensitive patient health information from being disclosed without

the patient's consent or knowledge. In the employment context, it is a best practice to keep an individual's health information private. If the employer is a covered entity, the HIPAA privacy rules prohibit the release of protected health information by others without consent. Therefore, to be in compliance with both EEOC guidelines and HIPAA, employers should have a policy that includes obtaining written consent from employees about releasing their vaccination documentation.

Verification of Vaccination Records

With the recent increase in the number of employers that are mandating their employees be vaccinated and provide proof of vaccination, this presents an incentive for individuals to create or doctor vaccination records. Employers have begun seeing an increase in suspicious or fraudulent vaccination records. This raises an important question. Is there a method employers can use to validate employee proof of COVID-19 Vaccination?

At a very fundamental level, determining the authenticity of a paper document, with no embedded security features, such as those which exist in currency, can be difficult. The CDC – COVID Vaccination Record Card, is a such document, and just like drivers' licenses, and other identification documents, for those looking to misrepresent their date of birth or vaccination status, a black market exists to purchase these cards. Recent seizures by law enforcement authorities of counterfeit CDC cards, and the illegal sale of genuine cards comes as no surprise to seasoned fraud investigators. In one case, a state data base of records were falsified to support a counterfeit card scheme. That being said, various methodologies do exist as best practices to determine the authenticity of the CDC-COVID Vaccination card.

The first method is to compare the CDC-COVID Vaccination card against a card known to be genuine, looking for inconsistencies in the symbols, dates, or language/terms used. Also, when examining the card, attention should be given to the manufacturer and timeline of doses. As we know, Moderna and Pfizer are double-dose vaccines administered several weeks apart, while J&J is a single dose vaccine. Other possible indicators may come to light if a novice is producing the fake or altered document, such as a combination of similar handwriting for both doses of a two-dose vaccine, same color pen, same dates for multiple shots, strike-throughs, smudges or scratch-outs. Typically, it is a combination of errors, rather than one deviation which may raise suspicion.

When the initial review of a card leads an employer to be suspicious, especially in the circumstance of less sophisticated fraudsters, there are additional steps the employer should take. In New Jersey and other states, a person's official vaccine status can be validated by the use of State-supported application on a mobile device. This typically is a much more reliable method for verification. We are recommending that employers request the vaccination card, and then validate the card through the corresponding application, in New Jersey the application is called Docket. It can be easily downloaded from the App Store, or Google Play Store. This method is preferable because the employee can use a company device, assigned to HR for example, downloaded on a tablet or mobile phone. The employee will need to provide the mobile phone number and email address, which was provided at vaccination, to locate the record. In the case of New Jersey's Docket, a digital record will appear, and a letter from the state in .pdf is available for review and download. The .pdf, contains the employee's date of birth, although personally identifiable information (PII), typically information already known by an employer. At the end of the session or periodically, an employer can delete the account, and the record, as a best practice to address any perceived data privacy concerns, and simply reload the application once more. This approach relieves the employer of hard document examination, especially when more sophisticated methods are employed to falsify a document, while minimizing data privacy concerns.

Takeaways

Employers are required to keep COVID-19 vaccination records confidential by creating a medical file into which the COVID-19 related medical information should be stored. This should be kept separate from the employee's personnel file. Alternatively, create a single file to store COVID-19 related documentation for all employees. Electronically submitted

documentation should not be stored on a system where others have access. A manager may use initials or another code to ensure confidentiality of the name of an employee. Consider requiring employees to submit vaccination records to a designated email address where access is restricted. Rather than collecting vaccination cards, an employer may opt to inspect the cards so as not to trigger retention obligations.

If employers have any concern over the authenticity of an employee's vaccination record, they can employ a number of tactics to validate, including careful review, follow up conversation with the employee to verify certain details (such as dates and location of administration), and finally requesting access to Docket or other State-administered vaccination database.

When an employer has done this and has determined that an employee has submitted a fraudulent card, the employer is permitted to discipline the employee up to and including termination. This discipline may be subject to compliance with specific state statutes or collective bargaining agreements or employment contracts, so it is advisable to seek legal guidance if an employee is suspected of presenting a fraudulent card.