The Federal Trade Commission Releases Guidance about Collection of COVID-19 Related Health Information

May 2, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Andrew Spital | Amelia Putnam

The Federal Trade Commission ("FTC") recently published guidance concerning COVID-19 ("COVID") related personal data that companies have collected during the COVID pandemic.[1] As people have returned in person to offices and events, many businesses have been asking their employees and customers to provide verified proof of their vaccination status.[2] In addition, to assist individuals in digitally storing information about their vaccination status, some companies developed "vaccine passport" apps that allow individuals to store certain COVID related personal data in digital wallets on their devices.[3] These apps can collect a variety of personal data, including information about an individual's vaccination status, name, date of birth, zip code, email address, and phone number.[4]

While this data in this context is often not subject to the privacy or security requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), the FTC guidance makes clear that collection of any sensitive health information – including COVID related information – "should come with a 'Caution: Handle with Care' label."[5] In its

1 Megan Cox, *What the Pandemic Has Taught Businesses About the Collection of Health Information*, FTC (Apr. 25, 2022), here.

2 *See* Tyler Sonnemaker, *Big Tech Companies are Telling Their Employees to be Vaccinated Before Returning to the Office as the Delta Variant Spreads*, Insider (July 28, 2021), here.

3 Examples of these apps include CommonPass, VeriFly, VaccTrak, and Excelsior Pass Plus.

4 Megan Cox, *What the Pandemic Has Taught Businesses About the Collection of Health Information*, FTC (Apr. 25, 2022), here.

5 *Id.*

guidance, the FTC provides several considerations for companies that develop apps that collect such personal data as well as for companies that check people's vaccination status.

Companies that Develop Vaccination Verification Apps

The FTC recommends that companies that develop health related apps adhere to these guidelines:

- Make accurate representations about how people's personal data will be used and shared. Companies should review their publicly available privacy policies to ensure that the privacy policies accurately describe what personal data is collected, with whom the personal data may be shared, and any rights that individuals may have with respect to their personal data under various privacy laws. If a company is subject to laws such as the California Consumer Privacy Act, the company should have in place a procedure that allows individuals to submit consumer requests concerning their personal data. Companies should also ensure that other businesses that use their apps understand how the personal data will be used and shared.

- Regularly update the app to protect against new security vulnerabilities and also update the Company's privacy claims to ensure such claims remain accurate. Companies must notify app users of such updates.

- Minimize the personal data that is shared. The FTC noted that data such as names, dates of birth, email addresses, and types of vaccines may not be required to verify an individual's vaccination status. Therefore, companies should avoid collecting this personal data or other personal data if such data is not necessary to accurately verify an individual's vaccination status.

- Implement appropriate data security measures to protect the sensitive data stored on the app. The FTC cautioned that individuals often use vaccine passport apps on open Wi-Fi access points or lose devices containing the apps, so companies should protect the data with measures such as encryption.

- Understand applicable laws and regulations, especially when dealing with children's data or health data. Children's data and health data are categories of sensitive personal data, so companies should ensure that their privacy and data security practices comply with the heightened standards. In addition, companies should understand the applicability of laws such as the Children's Online Privacy Protection Act and HIPAA to ensure that they comply to the extent that any of their activities trigger the requirements and obligations of those laws.

- Prioritize privacy and data security in developing the app. The FTC points app developers to its "Start with Security" guide that provides information about best practices for data security[6] and the National Institute of

[6] *Start with Security: A Guide for Company*, FTC, here (last accessed Apr. 28, 2022).

Standards and Technology's ("NIST") Secure Software Development Framework.[7] This guidance addresses certain data security measures, including access controls to personal data, secure storage and transmission of personal data, oversight over vendors and service providers to ensure their compliance with a company's data security program and the protection of personal data under a company's control, and secure development of software.

Companies that Verify an Individual's Vaccination Status

Many companies verify employees' and customers' vaccination status, as part of general safety and health considerations or to comply with their obligations under applicable laws or emergency orders. The FTC provides several guidelines for companies to consider with respect to checking people's vaccination status:

- Consider why the company is checking customers' vaccination status, including whether such verification is required to comply with a legal obligation or to conduct contact tracing. Companies should ensure that the collection of COVID related personal data is consistent with its purpose. Therefore, a company should avoid using such personal data for other purposes, such as marketing, if those purposes have not been clearly communicated to consumers in the privacy policy or otherwise at the time of collection.

- Consider whether checking vaccination status requires the company to receive other personal data. A company should avoid requesting additional personal data from its employees or customers if such data is unnecessary to verify their vaccination status. If the company does collect personal data, the company must also consider how long the data will be retained and how it can protect and securely store the data.

- Thoroughly research available apps on the market to better understand how each app works, what personal data it collects, and whether the representations made by the company align with the app service provider's practices. Companies should ensure that the app service provider has implemented data security measures to adequately protect sensitive personal data. Companies should also consider whether they should include specific contractual language in contracts with the service providers that addresses privacy and data security compliance. Indeed, specific contracts may be required under certain laws, including HIPAA, if applicable.

- Use the return in person to events and work environments as an opportunity to evaluate the company's general practices for processing personal data. Companies should consider whether they collect more personal data than is needed for business purposes and investigate whether they can improve their data security practices.

Additionally, if companies collect COVID related personal data and vaccination information from their employees, they should treat such personal data as confidential employee medical information that is stored separately from personnel

[7] *Secure Software Development Framework*, NIST, here (last accessed Apr. 28, 2022).

files. Companies should implement technical and administrative measures to protect such personal data from disclosure and ensure that it is not used for any purpose other than to comply with the company's COVID related policies.

Conclusion

For companies that collect COVID related health data to comply with legal requirements or otherwise to protect the health of their employees and customers, and companies that develop apps to help individuals store and track this personal data, the treatment and handling of sensitive health data cannot be an afterthought. The FTC has signaled that regulating the collection and use of individuals' COVID related personal data is one of its priorities. Companies that collect this personal data should carefully review their privacy and data security practices to ensure that such practices align with the FTC's guidance.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Andrew Spital
212 728 8756
aspital@willkie.com

Amelia Putnam
202 303 1089
aputnam@willkie.com