LeClair & Associates

Newsletter: October 5, 2021

Digital Proof of Vaccination Certificates: Cyber Security and Privacy Insights from our In-house Expert, Ritesh Kotak

- **At a glance:** In consideration of the Government of Ontario's plans to roll out a QR (Quick Response) code based digital vaccine certificate in late October, employers would be wise to ensure they do not subject themselves to unnecessary legal exposure from a privacy and cyber security standpoint.

- **What Exposure?** Given the highly sensitive Personally Identifiable Information ("PII") stored in vaccine certificate apps, employers may face costly litigation and fines for breaches of employee and customer data, as well as open themselves up to potential cyber security breaches given the attack vectors available to anyone who gains access to PII such as emails, phone numbers, addresses, and even government-issued heath cards or drivers licenses. This information in the hands of bad faith actors is something all employers should seek to avoid.

So, what steps can employers take to mitigate exposure?

- **Ask the right questions:** Employers must direct the below key queries to any prospective third-party company offering a digital proof of vaccination service.

- **Where is the data housed?** It is of paramount importance to inquire as to where the PII will be stored, and specifically whether the information is stored in Canada. A company storing PII outside Canada may preclude employers from recourse to the protections afforded by Canadian privacy legislation such as the ***Privacy Act***, and the ***Personal Information Protection and Electronic Documents Act (PIPEDA).*** Cross border data transfer may lead to the interception of data by entities outside Canada.

- **Is the Data encrypted?** There is perhaps no more important question to ask then whether the data stored in the third-party app will be encrypted. Encryption is the process of encoding information, usually concealing data in its original form (plaintext), into a cypher or hash value. Only authorized parties can revert the encrypted information into its plaintext form. Accordingly, encryption prevents unauthorized parties from utilizing data in the event of a cyber security breach. All employers interested in implementing or contracting with a digital vaccine certificate app should ensure that the app encrypts any stored data.

- **Can the data be manipulated?** Not all manipulation of data is a bad thing. Some data may be manipulated in order to increase ease of use and organization of data, however, some manipulation can be harmful (and costly). For example, hackers may breach an app's firewall and scramble the information of different profiles within the app. This may result in business continuity disruptions, and in the worst case, a complete cease in the operationality of an app.

- **How can one prevent manipulation of the data?** Employers should inquire whether a *penetration test* has been performed on any app they intend to use. A penetration test is a simulated cyber attack (white-hat hack) against your computer systems to check for exploitable vulnerabilities. These tests help prevent breaches before they happen; they are crucial to ensuring an apps security.

- **Will the data be repurposed?** Employers should also inquire to what end the data will be used upon its storage. Certain companies may indicate in their Terms of Service Agreement that data will be stored and then sold in the future. Ensuring that data stored is not sold will ensure employers do not expose themselves to the financial and reputational harms which accompany such privacy breaches. Not to mention, pursuant to *PIPEDA,* any such breach of personal information must be reported to the Office of the Privacy Commissioner or severe penalties may be imposed.

"This sounds very futuristic, are you sure these concerns impact our business right now?"

- **Pressing and immediate:** The case *Portpass,* the Calgary based proof of vaccine app, has recently demonstrated the severe outcomes of failure to make the inquiries we have outlined herein. With more than 650,000 users, *Portpass* has recently garnered national headlines for its security shortcomings whereby private data, including driver's licenses and health cards, were not stored securely. Just before this breach, The NHL's Calgary Flames had recommended that all fans attending games download the app to remove the friction associated with proving vaccination status with paper receipts and physical identification cards. While this is a worthy objective, the Flames lack of cyber hygiene has resulted in otherwise avoidable legal exposure.

- **We hope that the strategies herein will help your business assess the risk-vectors associated with digital vaccine apps and the sweeping digitization of business in the age of COVID-19.**

We will continue to share updates and insights in the coming weeks however, for specific questions, please feel free to reach out to us directly at –

ritesh@leclairandassociates.ca
nic@leclairandassociates.ca
(519) 859 6015