Privacy Commissioner
Bermuda

18 March 2020

Guidance on Privacy Issues in Public Health Emergencies

The modern approach to addressing emergencies has data at its heart. In situations that involve health and infectious disease, data on who might be infected, how they became infected, what their symptoms are, and with whom they have met could be important to contain the spread. Employers and other organisations may wonder how to balance privacy with their other responsibilities.

The Personal Information Protection Act 2016 (PIPA)[1] takes the approach that organizations should consider the risk of harm to an individual from collection, use, and disclosure of their personal information. Privacy of the individual, and the ability of that individual to control what happens to their data, must by necessity be balanced against other factors. Often, this balance is discussed in the context of freedom of speech or domestic use of data.

Today, the balance between privacy and public health is on all of our minds. PIPA provides exemptions for, among other matters: national security, emergencies, and for the protection of the health, safety, and welfare of individuals at work. In each of these use cases, organisations must still meet the law's Minimum Requirements, which require that organisations adopt suitable and reasonable measures, act in a fair and lawful manner, use only proportional information, maintain information's integrity, and implement security safeguards to protect it.

These requirements are flexible, allowing organisations to consider the type of data they are collecting, the risk of harm to the individual if that data is misused, and the purpose that they hope to accomplish. As such, the rules of PIPA would not prevent the use of personal information during public health emergencies, as long as the information is collected, used, and disclosed thoughtfully and with due care.

Employers, particularly, may be unsure about how to approach their responsibility to protect the safety of their employees in the context of privacy. With that in mind, here are a few frequently asked questions:

What kind of information can employers collect from their employees?

Employers may have a duty to take certain steps to protect the health and safety of their employees. It may be relevant to ask whether employees have engaged in international travel or are experiencing certain symptoms. As with any purpose for collecting data, an organization should identify in advance what the purpose for collecting or using specific pieces of information may be. In other words, for each question or line item, consider what specific task you may accomplish using that data, and why that particular amount of detail is needed. Organisations should consider what information would be the minimum necessary to accomplish their goal.

May employers share personal data relating to employees' health or travels?

Sharing personal information is a form of data use, so organisations must consider what purpose they will accomplish from such a use and in what detail they must share data to accomplish that purpose. For example, if an employer learns that an employee recently returned from an infected area, they may wish to warn other employees so that their employees may protect their own health. The employer may not need to reveal the individual or place of travel, and may only need to instruct

[1] As of the writing of this memo, relevant sections of PIPA have not yet entered into force pending an implementation timetable to be announced. Please consider this memo to be guidance on best practices.

colleagues to work separately. Consider the minimum amount of information that must be disclosed to accomplish the intended purpose.

Any organisation with relevant health or travel information should also consider whether sharing that information with public health authorities would be more prudent than choosing to disclose the information themselves.

What potential harms to individuals should employers consider when collecting, using, or disclosing personal information?

In situations of public health emergencies, emotions may be running high. Personal information could be abused, leading to unfounded accusations of personal responsibility for infections or other mistaken finger-pointing. Individuals may be unfairly discriminated against based upon their travel history or health.

Revealing health details about an individual may cause embarrassment or other harm. A person who contracted and recovered from the COVID-19 virus may be unfairly discriminated against. An individual with an underlying condition that could make the virus riskier for them may have higher insurance premiums or other consequences if that condition becomes public. If details such as an individual's known locations or associations become publicised, the community might engage in wild theories or speculative gossip about that individual.[2]

Information should only be collected, used, or disclosed after due consideration of the potential harms.

How should employers protect any data they collect?

Organisations should always implement appropriate safeguards to protect data against the specific risks that those particular pieces of information may pose. They should ensure that decisions are not made ad hoc or arbitrarily. Instead, procedures should be in place that describe exactly how staff should collect, store, and share any data, whether in paper or digital form. Security controls, such as locked file cabinets or password-protected computer files, should be utilised to ensure there is no malicious or even accidental access. Consider how data is transferred or transported, and whether that method is secured. Consider how to log access and custody of data.

Everyone who has access to potentially sensitive information should understand their responsibility to keep information confidential. Human Resources policies should govern employee behaviours and ensure employees may be held responsible for violations of these rules in accordance with other misbehaviour procedures.

What should I do if I have more questions?

Like many other organisations, the staff of the Office of the Privacy Commissioner will be working remotely for the near future, practicing socializing-at-a-distance. However, we will still be available to consult with the community on privacy topics. If you have questions, you may reach the Office by email at PrivCom@privacy.bm or by calling 543-PRIV [-7748], or you can follow the Office on social media at: https://www.linkedin.com/company/PrivComBermuda.

Alexander McD White
Privacy Commissioner

[2] For more on this topic, see: http://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives