Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic

Introduction

During the COVID-19 pandemic, especially since the onset of the fifth wave in early 2022, organisations in Hong Kong have been deploying epidemic prevention and control measures in the workplace to ensure the health and safety of employees. Health data of employees is normally collected by employers, with a view to introducing effective anti-epidemic measures to reduce the risk of transmission of coronavirus variants in the workplace. **This guidance note is issued to help employers and employees in Hong Kong to understand the employers' obligations under the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) ("PDPO") when it comes to the collection and use of employees' health data in the context of the COVID-19 pandemic.**

The PDPO contains no definition of the term "health data". In the context of the COVID-19 pandemic, health data generally refers to personal data which reveals information of an individual's health status in relation to COVID-19. This may include information regarding whether an individual has been vaccinated against COVID-19, tested positive or negative of COVID-19, and/or recovered from COVID-19.

1. Can an employer collect temperature measurements, travel histories, vaccination records, COVID-19 test results, infection records and other COVID-19 related health data from employees?

Employers in Hong Kong are under both a statutory duty[1] and a common law duty to, so far as it is reasonably practicable, ensure the health and safety at work of the employees. Aside from legal obligations, organisations are generally expected to also protect the health of their visitors as part of their corporate social responsibility.

Against this background, it is generally justifiable and reasonable for employers to collect temperature measurements[2], travel histories, vaccination records, COVID-19 test results, infection records and other COVID-19 related health data from employees, so that the employers can assess the risk of transmission of the coronavirus in the workplace and safeguard the health of employees and visitors during the pandemic.

1 Pursuant to section 6(1) of the Occupational Safety and Health Ordinance (Cap. 509 of the Laws of Hong Kong), every employer must, so far as reasonably practicable, ensure the safety and health at work of all the employer's employees.

2 If an employer uses temperature scanners to check employees' temperatures without recording their temperature readings, the data in question (i.e. temperature readings as appeared on scanners temporarily) is not "personal data" as defined under the PDPO. When no personal data is collected, the PDPO will not apply.

From the perspective of the protection of personal data, it is noteworthy that employers should only collect health data that is necessary for or directly related to the purposes of collecting the data[3]. Personal data irrelevant to or not strictly necessary for the prevention or control of COVID-19 in the workplace should not be collected. Employers should consider the specific circumstances of the organisation and the workplace, and determine whether the collection of certain kinds of health data is necessary in those circumstances. For brick-and-mortar organisations that provide face-to-face customer services (such as retailers and eateries), generally it would be reasonable and necessary for employers to collect employees' vaccination records (or valid proof of medical exemption), COVID-19 test results and infection records with a view to making suitable operational arrangements. This is particularly so for catering businesses which are subject to Vaccine Pass arrangements, as all staff on the catering premises under certain modes of operations must have received at least one dose of vaccine, unless they have been issued with a COVID-19 Vaccination Medical Exemption Certificate.

The principle of data minimisation should be applied. Personal data collected by employers should be adequate but not excessive in relation to the purpose for which it is collected[4]. Subject to operational feasibilities and other relevant considerations, the least privacy intrusive measures should always be adopted. For example, employers should avoid using devices with image recording function for temperature checks. Employers should consider adopting a self-reporting system and collecting the relevant health data through questionnaires which provide multiple-choice answers. Open-ended questions should be avoided lest unnecessary personal data be collected inadvertently.

The manner in which health data is collected also matters. Personal data from employees shall only be collected by means which are lawful and fair in the circumstances. Employers cannot, for example, collect employees' health data by deception, intimidation, or undue influence.

2. Can an employer collect the health data of an employee's family member(s)?

Generally speaking, in order to safeguard the health and safety of employees at work, and to ascertain employees who are close contacts of confirmed cases or who are subject to quarantine orders, it is justifiable and reasonable for employers to request employees to notify them if the employees are close contacts of confirmed cases or are subject to quarantine orders. Under most circumstances, however, collection of the health data of an employee's family member(s), such as their vaccination records, will not be considered necessary or proportionate.

In this context, employers are reminded that they should only collect health data that is necessary for or directly related to the purposes of collecting the data, and the data collected should be adequate but not excessive in relation to the purpose for which it is collected.

3. What do employers need to tell employees when they collect health data from employees?

Under Data Protection Principle ("DPP") 1(3), on or before collecting personal data, employers shall take all practicable steps (such as by way of notice) to inform the employees of, among others, the purposes of collection (such as safeguarding the health of employees and visitors / customers), the classes of persons (such as public health authorities) to whom the data may be transferred, and whether it is obligatory or voluntary to provide the personal data. As a matter of good practice, employers should also inform employees of the

3 Data Protection Principle 1(1)(b) provides that personal data shall not be collected unless the collection of the data is necessary for or directly related to that purpose.

4 Data Protection Principle 1(1)(c).

retention period of the data[5]. DPP 5 requires that information about the data user's policies and practices should be made generally available. Employers should be transparent and open with employees as to why they need to and how they would collect and process the employees' health data.

The Office of the Privacy Commissioner for Personal Data ("PCPD") recommends that employers clearly convey all the requisite information to employees, such as by presenting a Personal Information Collection Statement ("PICS"), unless the employers' existing privacy notices already cover the relevant information. The PICS should cover, for example:

- whether the submission of the health data is obligatory or voluntary;
- the consequences if the employees fail or refuse to provide the data;
- the purpose(s) for which the data is to be used (e.g. complying with the relevant statutory requirements or making suitable operational arrangements such as arranging for staff members who are tested positive for COVID-19 to take sick leave);
- who (or the rank of officers) may have access to the data;
- to whom the data may be transferred, and what kinds of data may be transferred; and
- how employees may access their health data and seek correction.

4. Can employers use the health data of employees for other purposes or disclose the data to other parties?

Health data collected from employees should only be used for the original purposes that they were informed of (such as safeguarding the health of employees at work) or directly related purposes. **Under DPP 3, employers must obtain the "prescribed consent" (i.e. voluntary and express consent) of employees before using the relevant data for a new purpose, including disclosing the data to other parties for a new purpose.**

The PDPO allows certain situations under which the use and disclosure of personal data may be exempted from seeking the prescribed consent from the data subjects (i.e. employees in the present context). The situations relevant to the COVID-19 pandemic may include, for example, (1) the disclosure of the identity, health and location data of employees to public health authorities for tracing and treating persons infected with COVID-19 and safeguarding public health[6]; and (2) the use or disclosure of employees' personal data for compliance with the requirements of laws (such as the Prevention and Control of Disease (Disclosure of Information) Regulation, Cap. 599D of the Laws of Hong Kong)[7].

If an employee has tested positive for COVID-19, the employer may notify other staff members, visitors and the property management office without disclosing any personally identifiable information of the infected person. For example, it is generally sufficient for the employer to issue a notice with information that a staff member has been infected. Under most circumstances, disclosure of the name and other personal particulars of an infected person in the notification will not be considered necessary or proportionate.

5. How long can employers keep the health data collected by them?

Generally speaking, employers should not retain the health data for a period longer than is necessary[8]. When the purpose of collection is fulfilled, the employer should permanently destroy the personal data collected for combatting COVID-19. In this regard, employers may, if necessary, refer to the information

5 Please refer to Question 5 below for the "retention period" of personal data.
6 Sections 59(1)(b) and (2) of the PDPO.
7 Section 60B(a) of the PDPO.
8 DPP 2(2) requires a data user to take all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

provided by the public health authorities on the common incubation period for COVID-19.

In the event that the employment relationship is terminated, all the health data of the former employee should be erased as soon as practicable, subject to any legal or contractual obligations that the employers are obliged to fulfil. For practicable guidance on matters in relation to the handling of the personal data of former employees, employers may refer to section 4 of the Code of Practice on Human Resources Management[9] published by the PCPD.

6. How can employers make sure that the health data collected is accurate? How frequent should employers seek to update the health data?

DPP 2(1) requires data users to take all practicable steps to ensure that personal data is accurate having regard to the purposes for which it is collected. If employers believe that any of the information is incorrect or outdated, they should seek clarification from employees.

Insofar as vaccination status and COVID-19 test results are concerned, employers should ensure that policies and systems should be in place to maintain accurate and up-to-date vaccination information and test results of employees. This could be achieved by, for instance, requesting a staff member to report the latest vaccination status within a certain number of days after the staff member was inoculated, or report the test result within a reasonable period after the staff member was notified of the result.

7. What should employers be mindful of in relation to data security?

Health data is generally considered sensitive. If the data is leaked, it may cause significant harm (including psychological harm) to the relevant persons. Hence, data security is of particular importance in this context. **Under DPP 4(1), employers should take all practicable steps to ensure that the personal data collected is protected against unauthorised or accidental access, processing, erasure, loss or use.** This includes:

- in the case of paper records, storing the paper records in a locked cabinet and keeping the paper records out of public sight;
- in the case of electronic records, encrypting digital data and using passwords to protect electronic devices that contain health data; and
- limiting access to authorised personnel and allowing access only on a need-to-know basis.

To prevent the health data of an employee from being viewed by or leaked to other staff members, employers should not arrange for the employees to report the data on any shared form (in the case of paper records) or upload the information to, for example, a centralised electronic platform, an instant messaging / communication platform or application or a shared document on the cloud to which access is available to all other staff.

If a data leakage occurs, the employer should consider notifying the staff member concerned, the PCPD and other law enforcement agencies as soon as possible.

9 The Code is available at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf.

8. What are the rights of employees in relation to their personal data?

As personal data belongs to the data subjects, employers should handle the employees' personal data in a respectful and prudent manner. Under DPP 1(3)(b)(ii), employers should, on or before the first use of the data, inform employees of their rights to request access to and the correction of the data, and provide the name and contact information of the staff member responsible for handling such requests. **In this context, DPP 6 expressly provides employees with the right to request access to and correction of their own personal data.**

9. Are there any other matters that employers should note in relation to the handling of the personal data collected from employees?

Employers are also reminded to comply with the requirements of the Code of Practice on Human Resources Management[10] published by the PCPD. The Code covers issues concerning the collection, holding, accuracy, use and security, and data subject's access and correction requests in relation to the personal data of prospective, current and former employees.

10. Where can employers and/or employees make enquiries or complaints about the handling of the personal data of employees?

For enquiries or complaints in relation to the handling of the personal data, including health data, of employees, employers and/or employees may get in touch with the PCPD at 2827 2827, or communications@pcpd.org.hk for making an enquiry and complaints@pcpd.org.hk for filing a complaint[11].

10 See footnote 9.

11 According to section 37 of the PDPO, a complaint must be lodged in writing in Chinese or English or in another form accepted by the Commissioner, and the act and/or practice complained of and the data user involved must be specified. Please visit the PCPD's website at https://www.pcpd.org.hk/english/complaints/how_complaint/complaint/complaint.html for downloading the complaint form.

Summary of Recommendations:

- **Necessity:** Employers should only collect the health data that is necessary for and directly related to the purpose(s) of data collection. Personal data irrelevant to or not strictly necessary for the prevention or control of COVID-19 in the workplace should not be collected.

- **Data minimisation:** The data collected by employers should be adequate but not excessive in relation to the purpose(s) for which it is collected. The least privacy intrusive measures should be adopted.

- **Transparency:** Employers should clearly convey all the requisite information to employees, such as by presenting a Personal Information Collection Statement.

- **Retention and erasure:** Employers should not retain the health data of employees for a period longer than is necessary. When the purpose of collection is fulfilled, the employer should permanently destroy that data.

- **Accuracy:** Employers should ensure that policies and systems be in place to maintain accurate and up-to-date vaccination information and test results of employees.

- **Security:** Employers should take all practicable steps to protect the health data collected against unauthorised or accidental access, processing, erasure, loss or use, such as by locking paper records, encrypting electronic records, and limiting data access to authorised personnel on a need-to-know basis.

PCPD website

Download this publication

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **Room 1303,13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

March 2022