

CHAPTER 4

INFORMATION SHARING AND CONFIDENTIALITY

GOVERNING PRINCIPLES

4.1 Professionals should protect the confidentiality of the personal data of their clients obtained in the course of their duties because privacy is protected both legally and ethically – Article 14 of the Hong Kong Bill of Rights, Personal Data (Privacy) Ordinance, the Common Law and the professionals code of ethics. However, in exceptional cases, depending on the circumstances, disclosure may be justified when disclosure of information is necessary to prevent foreseeable harm to a child.

The Common law duty of confidentiality

4.2 The courts recognize that professionals such as social workers and lawyers owe a duty to those who consult them to keep information they have learned about them confidential. If they breach such duty without justification, the court can interfere by making an award for damages or an injunction prohibiting disclosure of the relevant information. Whilst the starting point is that the source of a social worker's information is confidential, there may be circumstances which justify disclosure. The role of the social workers is to balance the interest in maintaining confidentiality and the interest in breaching confidentiality. Such circumstances includes where disclosure is in the interest of the client or the person who gave the information – the “need to know” exception.

4.3 To protect a child from being abused, sharing of information among relevant professionals on a need-to-know basis is essential to facilitate risk assessment and timely and appropriate intervention.

4.4 Relevant information relating to child protection may include :

- (a) health and development of a child and his/her exposure to possible harm;
- (b) child care ability of a parent / carer that may pose danger to the child under his/her care;
- (c) act that may cause harm to a child; and
- (d) actual harm to the child.

4.5 The Personal Data (Privacy) Ordinance, Cap 486, should be complied with in sharing information.

4.6 The principles that a medical practitioner is required to observe with regard to patient confidentiality and disclosure of medical information are at Annex I to Chapter 4.

4.7 The principles that a clinical psychologist, who is a member of the Hong Kong

Psychological Society, is required to observe in regard to communication of information on clients are at Annex II to Chapter 4.

- 4.8 The principles that a social worker is required to observe under the Code of Practice for Registered Social Workers are at Annex III to Chapter 4.

PERSONAL DATA (PRIVACY) ORDINANCE, CAP 486

- 4.9 The sharing of personal data is governed by the Personal Data (Privacy) Ordinance, Cap 486 [PD(P)O] which controls the collection, holding, processing and use of personal data by data users and enables an individual to request access to and correction of any personal data relating to him/her. In collecting data and sharing information, professionals should observe the data protection principles as stipulated in Schedule 1 of the PD(P)O :

Principle 1- Purpose and Manner of Collection of Personal Data

Principle 2 - Accuracy and Duration of Retention of Personal Data

Principle 3 - Use of Personal Data

Principle 4 - Security of Personal Data

Principle 5 - Information to be Generally Available

Principle 6 - Access to Personal Data

(Details of the Data Protection Principles are at Annex IV to Chapter 4.)

PRINCIPLES OF SHARING OF INFORMATION

- 4.10 According to Data Protection Principle 3, data user should not use (including disclose or transfer) personal data for any purpose other than the purpose for which the data were to be used at the time of collection or a directly related purpose unless the data subject's prescribed consent is obtained.
- 4.11 The PD(P)O allows use, disclosure or transfer for a different purpose and without the data subject's consent where the use, disclosure or transfer is exempted from the provision of Principle 3 by virtue of Part VIII of the Ordinance - Exemptions.
- 4.12 Section 58 of the PD(P)O provides an exemption from Principle 3 where the observance of the provisions of Principle 3 would be likely to prejudice the detection or prevention of crime or the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct. As such, Principle 3 may be invoked if the data are to be used and shared for the purpose of child abuse investigation or related child protection work.
- 4.13 According to Section 59 of the PD(P)O, personal data relating to the physical or mental health of the data subject may be exempted from Principle 3 if application of this Principle would likely cause serious harm to the physical or mental health of the data subject or any other individuals. Claiming this

exemption, professionals (e.g. medical practitioners, residential child care staff) may share health record of service users, including suspected abusers and victims of child abuse, with other concerned professionals on a need-to-know basis for the purpose of protecting a child from serious physical and/or mental harm.

- 4.14 In handling request for access to personal data under Data Protection Principle 6, as stipulated in Section 58(1)(a), (b) & (d), Section 59(a) of the PD(P)O, exemption from access and correction may be invoked provided the data user has reasonable grounds for believing that release of the personal data (which were held for child abuse investigation and related child protection work) would likely prejudice the investigation and any possible proceedings on a suspected child abuse case and protection for the child.
- 4.15 If any person (including a child victim) makes a disclosure of a suspected child abuse incident and asks for it to be kept secret, it should be explained to the person that it is in the best interest of the concerned child that such a promise cannot be made.

MEASURES TO PRESERVE CONFIDENTIALITY

- 4.16 While exemption from Data Protection Principle 3 on the use of data may be invoked in circumstances as mentioned in paragraphs 4.9 to 4.10 above, in all circumstances, professionals should disclose the least amount of confidential information necessary to achieve the desired purpose and only information that is directly relevant to the purpose for which the disclosure is made should be revealed.
- 4.17 Confidential information should not be discussed in any setting unless confidentiality can be ensured. Hence, discussion in public or semi-public areas such as hallways, waiting rooms, elevators and restaurants should be avoided.
- 4.18 All professionals should take precautions to ensure and maintain confidentiality of information transmitted to other parties through the use of computers, electronic mail, telephones and telephone answering machines, and other electronic or computer technology such as message left through pager service. Disclosure of identifiable information should be avoided whenever possible.
- 4.19 All professionals should not disclose identifiable information of any service user in the course of discussion for teaching or training purposes or seeking advice from a third party outside their organisation unless the service user has consented to the disclosure of confidential information.
- 4.20 All professionals should protect the confidentiality of service user(s) according to the preceding principles even after the case has been closed.

CHILD PROTECTION REGISTRY (CPR)

- 4.21 The CPR is a computerized record system which carries the function of case registration, case checking as well as facilitating statistical research. The main objectives of the CPR are :
- (a) to facilitate better communication among government departments and NGOs, which are registered users handling child abuse cases, through an easy checking mechanism to ascertain whether a case is a known case of any department / organisation;
 - (b) to collect and compile statistical information on the abused children and their abusers in known and/or at risk cases of child abuse for the purpose of ascertaining the magnitude of the problem, including identification of the general profile and characteristics of child abuse;
 - (c) to monitor regular updating and review of significant data to ensure accuracy of the statistical information as far as possible; and
 - (d) to facilitate planning and development of services which prevent child abuse, including planning of public education programmes to prevent child abuse.

(Reference can be made to Appendix VI for information on CPR.)

- 4.22 All SWD & NGO service units providing casework service including Integrated Family Service Centres, Integrated Services Centre, Family and Child Protective Services Units, Medical Social Services Units, Probation Offices, School Social Work Units, Outreaching Social Work Units, Integrated Children and Youth Services Centres, etc. are requested to report child abuse cases and children at risk of abuse to the CPR. Through the checking mechanism, registered users (including Officers-in-charge / Supervisors / Social Work Officers of service units from both SWD and NGOs as listed in this paragraph, senior medical officers / medical officers-in-charge, as well as designated police officers of the Child Abuse Investigation Units (CAIUs) of Hong Kong Police Force) may check whether a case is a known case of any department / organisation.
- 4.23 Apart from keeping record of the reported cases and providing case checking function, annual statistical report to provide information on the general profile of the newly reported child abuse cases is produced.
- 4.24 Although it is a good practice to inform the data subject of the transfer of his/her personal data to the CPR arguably, his/her prescribed consent is not required because :
- (a) if the purpose for which personal data of the victim and other individuals were collected by the reporting NGOs include the handling and investigation of, and the planning of services to prevent child abuse, and,

then it may be argued that the transfer of data to the CPR for use for the purposes as mentioned in paragraph 4.21 (a)-(d) is a purpose directly related to the purpose for which the data were collected; or

- (b) even if the purpose of disclosure of the data by the social workers of the NGOs to the CPR constitutes a purpose different from the purpose for which the data were collected by them, exemption from Principle 3 provided under Section 58 may be invoked by the NGOs if they have reasonable grounds for believing that investigation, detection or prevention of child abuse would be likely to be prejudiced if the data concerned were not reported to the CPR.

A list of frequently asked questions is at [Annex V to Chapter 4](#) for reference.

Medical Practitioners and Confidentiality Issues

Under *Duties of Doctors to the Sick* of the International Code of Medical Ethics (World Medical Assembly, 1983),

“[a] doctor shall preserve absolute confidentiality except where others are endangered on all he knows about his patient even after the patient has died.”

Under Section A, part III, of the Professional Code and Conduct for the Guidance of Registered Medical Practitioners (Medical Council of Hong Kong, 2000), a medical practitioner is required to observe the following principles in regard to patient confidentiality and disclosure of medical information :

1.4 Disclosure of medical information to third parties

- 1.4.1 A doctor should obtain consent from a patient before disclosure of medical information to a third party not involved in the medical referral.
- 1.4.2 In exceptional circumstances medical information about a patient may be disclosed to a third party without the patient's consent. Examples are: (i) where disclosure in the public interest or in the interests of an individual is justified because the failure to disclose the appropriate information would expose the patient, or someone else, to a risk of death or serious harm; (ii) when required by law to do so.
- 1.4.3 However, before making such a disclosure, a doctor must weigh carefully the arguments for and against disclosure and be prepared to justify the decision. If in doubt, it would be wise to discuss the matter with an experienced colleague or to seek help from a medical defence society, a professional association or an ethics committee.

In addition,

- 1.1.4 Doctors should be aware of the provisions of the Personal Data (Privacy) Ordinance (Cap 486), and have due regard to their responsibilities and liabilities under that Ordinance. In particular they should be aware of the patient's rights of access to and correction of the information in the medical record and the circumstances when these rights may be refused.

Clinical Psychologists and Confidentiality Issues

Under Chapter 8 of the Code of Professional Conduct (Hong Kong Psychological Society, 1998), a member of the Hong Kong Psychological Society is required to observe the following principles in regard to communication of information on clients :

- 8.1 Members who, in preparing a report, draw substantially upon the work of other professionals shall seek their consent to include such material and shall acknowledge its source in the report.
- 8.2 Test scores, like test materials, are released only to persons who are qualified to interpret and use them properly. Usually, an interpretation of the test results rather than test scores, is communicated.
- 8.3 The reporting of data obtained from test materials which are designed for self-appraisal purposes in schools, social agencies, or industry shall be closely supervised by Members, and provisions should be made for referring and counselling individuals when needed.
- 8.4 All psychological reports, whether oral or written, shall be directly concerned with the problems at issue and shall be expressed as simply and unequivocally as possible, with due regard for the understanding and qualifications of the recipient.
- 8.5 If an organisation employing a Member wishes to obtain psychological data about a client from another professional or another organisation, Members shall endeavour to establish the principle that they are the proper persons to obtain such information and to relay it to other workers within the organisation.
- 8.6 Confidential materials about clients or subjects, which might lead to their identification, shall not be released without their permission.

Social Workers and Confidentiality Issues

As stipulated in the “Principles of Practice Related to Clients” under the Code of Practice for Registered Social Workers (Social Workers Registration Board 1998),

“3. The social worker should inform clients fully, as far as possible, about the limits of confidentiality in a given situation, and the purpose for which information is obtained, and how it may be used. In publication of case material, the social worker should make necessary and responsible efforts to remove all identification information and to seek consent, as far as possible from client and the employing agency.”

The following sections are extracted from the Guidelines on the Code of Practice for Registered Social Workers (Social Workers Registration Board, 2000) for reference :

Guidelines :

- 3.5 Informed consent has to be obtained from the clients and the employing agency for the release of client’s information. If the social workers are of the view that the clients are not capable of making an appropriate decision, informed consent from the client’s guardians should be obtained. Social workers should make reasonable efforts to remove any information contained in the case material that may reveal the identity of the clients to someone who is casually related to the clients (e.g. neighbours, workmates, school teachers, etc.). If personal information of clients should be disclosed, the social workers should obtain the clients’ prior consent and assess whether the clients might have the ability to estimate the consequences of making such a decision.
- 3.6 In circumstances where there is sufficient evidence to raise serious concern about the safety or interests of clients or of others who may be affected by the clients’ behaviour, social workers should take such steps as are judged necessary to inform appropriate third parties even without the prior consent of the clients. Whether the social workers should alert the clients about going beyond the limits of confidentiality depends on the judgement of any reasonable person that the serious concern under consideration may exacerbate or transform into something even worse.
- 3.8 The clients have the right to know about the information relating to themselves that are being stored in their own case files and to access to the information that is provided by them or consequential to the information provided by them (e.g. opinions of the social workers, diagnosis, treatment plans, etc.). Information obtained from other sources, or their consequentials, should also be accessible to the clients and consent of the clients have to be sought before the relevant contacts are made, except when the clients have given up such a right prior to the social workers’ action to obtain such information. The access of the clients to such information may only be limited in the circumstances where there is sufficient evidence to raise serious concern that the safety or interests of clients or concerned persons will be jeopardized. If the guardians of the

clients wish to obtain information about the clients, they must first seek the consent of the clients. At the same time, the social workers must make a judgement as to whether or not the clients have the capability to make an appropriate decision and whether or not the decision so made is in the interests of the clients.

- 3.10 Should the social workers receive a request from the Police to provide personal information about their clients, the social workers should first seek the consent of the clients. When necessary, the social workers should make a professional judgment, after considering whether or not provision of the information would cause damage to the personal safety or interests of the clients or other people. If the Police hold a search warrant, the social workers should cooperate with the Police and provide information that is basic and necessary.

DATA PROTECTION PRINCIPLES

(extracted from Schedule 1 of the Personal Data (Privacy) Ordinance, Cap 486)

1. Principle 1 – Purpose and Manner of Collection of Personal Data

- (1) Personal data shall not be collected unless -
 - (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
 - (c) the data are adequate but not excessive in relation to that purpose.

- (2) Personal data shall be collected by means which are –
 - (a) lawful; and
 - (b) fair in the circumstances of the case.

- (3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that –
 - (a) He is explicitly or implicitly informed, on or before collecting the data, of –
 - (i) whether it is obligatory or voluntary for him to supply the data; and
 - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
 - (b) He is explicitly informed –
 - (i) on or before collecting the data, of –
 - (A) the purpose (in general or specific terms) for which the data are to be used; and
 - (B) the classes of persons to whom the data may be transferred; and
 - (ii) on or before first use of the data for the purpose for which they were collected, or –
 - (A) his rights to request access to and to request the correction of the data; and
 - (B) the name and the address of the individual to whom any such request may be made,

Unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2 – Accuracy and Duration of Retention of Personal Data

- (1) All practicable steps shall be taken to ensure that –

- (a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
 - (b) Where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used –
 - (i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or
 - (ii) the data are erased;
 - (c) Where it is practicable in all the circumstances of the case to know that -
 - (i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and
 - (ii) that data were inaccurate at the time of such disclosure, that the third party –
 - (A) is informed that the data are inaccurate; and
 - (B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.
- (2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 – Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than –

- (1) the purpose for which the data were to be used at the time of the collection of the data; or
- (2) a purpose directly related to the purpose referred to in paragraph (1).

4. Principle 4 – Security of Personal Data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to –

- (1) the kind of data and the harm that could result if any of those things should occur;
- (2) the physical location where the data are stored;

- (3) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
- (4) any measures taken for ensuring the integrity, prudence and competence to persons having access to the data; and
- (5) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 – Information to be Generally Available

All practicable steps shall be taken to ensure that a person can –

- (1) ascertain a data user's policies and practices in relation to personal data;
- (2) be informed of the kind of personal data held by a data user; and
- (3) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 – Access to Personal Data

A data subject shall be entitled to –

- (1) ascertain whether a data user holds personal data of which he is the data subject;
- (2) request access to personal data –
 - (a) within a reasonable time;
 - (b) at a fee, if any, that is not excessive,
 - (c) in a reasonable manner; and
 - (d) in a form that is intelligible;
- (3) be given reasons if a request referred to in paragraph (2) is refused;
- (4) object to a refusal referred to in paragraph (3);
- (5) request the correction of personal data;
- (6) be given reasons if a request referred to in paragraph (5) is refused; and
- (7) object to a refusal to in paragraph (6).

Frequently Asked Questions about Information Sharing and Confidentiality Issues

- 1. If a child has disclosed child abuse incident(s) to a professional (e.g. a teacher, a child care worker, etc.) and requested the professional to keep the information confidential and not to disclose the case to a third party, what should the professional do?**

It should be explained to the child that it is in his/her best interests that such a promise cannot be made although the child's concerns should be addressed. Instead, the professional should assure the child that the prime objective of any follow up actions is for his/her best interests. Moreover, timely risk assessment has to be made to secure prompt supportive service for the child.

- 2. Would verbal disclosure of relevant information of the child victims to other professionals relating to child protection violate the Personal Data (Privacy) Ordinance?**

- According to Data Protection Principle 3, data user should not use (including disclose or transfer) personal data for any purpose other than the purpose for which the data were to be used at the time of collection or a directly related purpose unless the data subject's prescribed consent is obtained.
- The Ordinance allows use including disclosure or transfer of personal data for a different purpose and without the data subject's consent where such use, disclosure or transfer is exempted from the provision of Principle 3 by virtue of Part VIII of the Ordinance - Exemptions.
- Section 58 of the Ordinance provides an exemption from Principle 3 where the observance of the provisions of Principle 3 would be likely to prejudice the detection or prevention of crime or the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct. As such, Principle 3 may be invoked if the data were to be used and shared for the purpose of child abuse investigation or related child protection work.

- 3. How can the medical officer-in-charge get access to the CPR?**

Medical officer / medical officer-in-charge can register as "user" of the CPR to gain access to the CPR checking system. They should forward the particulars of the office and the authorized officer to the CPR by completing the Record Form for Access at Annex 1 to Appendix VI. Whenever there are changes, updating is required.

4. Can the medical officer-in-charge, with reasonable suspicion, check the CPR before initiation of child protection mechanism?

Yes, provided that the medical officer-in-charge is a registered user of CPR.

5. What kind of information should be provided in giving statement to the Police?

In handling reports of child abuse, the paramount concern of the Police is to protect the safety and best interest of children, especially the abusers are often their close relatives or caregivers. To this end, the Police would conduct thorough investigation to gather evidence including the testimonies of victims and witnesses, case exhibits, medical/forensic evidence as well as any other circumstantial evidence, so as to establish the authenticity of the allegation. Where there is evidence of an offence, the abuser would be arrested. For the Police to initiate prosecution actions against the abuser, it is crucial to have sufficient evidence and the testimonies are of particularly importance.

Since any first-hand information or direct knowledge of the alleged crime, the victim, the witness, the alleged abuser and even other related incidents, etc. would be of relevance to the investigation, the Police will ask the professional involved to give a detailed statement of these facts. As victims may tend to disclose certain information, which may be of material assistance to the investigation or the prosecution, to the professional at some stage during interviews or contacts, whether in person, by phone, in writing or otherwise, full particulars of these communications would be essential. The professional should provide the full records of such interviews / contacts, whether in the form of a written report, audio / video recordings or otherwise, including date, time, location, persons involved, purpose of the communications, process of the events, and personal observations, etc.

Part VIII of the Personal Data (Privacy) Ordinance (Cap 486) provides specific exemptions for collection and transfer of information. It is exempted from the data protection principle 3 under section 58(2) of the Ordinance to disclose to the Police the personal data of the victim, and any other persons relevant to the investigation, if the disclosure of information is related to the prevention / detection of crime, the arrest / prosecution of the offender or the preclusion / remedying of unlawful conduct, etc.