Health Records and Information Privacy Act 2002 No 71

[2002-71]

New South Wales

Status Information

Currency of version

Historical version for 13 January 2023 to 30 September 2023 (accessed 19 June 2024 at 2:36)

Legislation on this site is usually updated within 3 working days after a change to the legislation.

Provisions in force

The provisions displayed in this version of the legislation have all commenced.

Notes—

- **Does not include amendments by**
  Public Interest Disclosures Act 2022 No 14 (not commenced — to commence on 1.10.2023)

Authorisation

This version of the legislation is compiled and maintained in a database of legislation by the Parliamentary Counsel's Office and published on the NSW legislation website, and is certified as the form of that legislation that is correct under section 45C of the Interpretation Act 1987.

File last modified 20 January 2023

Health Records and Information Privacy Act 2002 No 71

New South Wales

Contents

Health Records and Information Privacy Act 2002 No 71

New South Wales

An Act to make provision for the protection of health records and information; and for other purposes.

Part 1 Preliminary

1 Name of Act

This Act is the *Health Records and Information Privacy Act 2002*.

2 Commencement

This Act commences on a day or days to be appointed by proclamation.

3 Purpose and objects of Act

(1) The purpose of this Act is to promote fair and responsible handling of health information by—

(a) protecting the privacy of an individual's health information that is held in the public and private sectors, and

(b) enabling individuals to gain access to their health information, and

(c) providing an accessible framework for the resolution of complaints regarding the handling of health information.

(2) The objects of this Act are—

(a) to balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information, and

(b) to enhance the ability of individuals to be informed about their health care, and

(c) to promote the provision of quality health services.

4 Definitions

(1) In this Act—

authorised representative has the meaning given by section 8.

Commonwealth agency means an entity referred to in paragraph (a)–(h) of the definition of ***agency*** in the *Privacy Act 1988* of the Commonwealth.

Commonwealth Privacy Commissioner means the Office of the Privacy Commissioner established by the *Privacy Act 1988* of the Commonwealth.

emergency has the same meaning as in the *State Emergency and Rescue Management Act 1989*.

exercise a function includes perform a duty.

function includes a power, authority or duty.

generally available publication means a publication (whether in paper or electronic form) that is generally available to members of the public, but does not include any publication or document declared by the regulations not to be a generally available publication for the purposes of this Act.

genetic information means health information of a type described in section 6 (d).

genetic relative means a person who is related to an individual by blood, for example, a sibling, parent or descendant of the individual.

guidelines means guidelines issued by the Privacy Commissioner as referred to in section 64.

health care means any care, treatment, advice, service or goods provided in respect of the physical or mental health of a person.

Health Care Complaints Commission means the Health Care Complaints Commission constituted by the *Health Care Complaints Act 1993*.

health information has the meaning given by section 6.

health privacy code of practice or ***code*** means a privacy code of practice relating to health information made under Part 5.

Health Privacy Principle or ***HPP*** means a clause of Schedule 1. A reference in this Act to a Health Privacy Principle by number is a reference to the clause of Schedule 1 with that number.

health service includes the following services, whether provided as public or private services—

(a) medical, hospital, nursing and midwifery services,

(b) dental services,

(c) mental health services,

(d) pharmaceutical services,

(e) ambulance services,

(f) community health services,

(g) health education services,

(h) welfare services necessary to implement any services referred to in paragraphs (a)–(g),

(i) services provided in connection with Aboriginal and Torres Strait Islander health practices and medical radiation practices,

(j) Chinese medicine, chiropractic, occupational therapy, optometry, osteopathy, physiotherapy, podiatry and psychology services,

(j1) optical dispensing, dietitian, massage therapy, naturopathy, acupuncture, speech therapy, audiology and audiometry services,

(k) services provided in other alternative health care fields in the course of providing health care,

(l) a service prescribed by the regulations as a health service for the purposes of this Act.

health service provider means an organisation that provides a health service but does not include—

(a) a health service provider, or a class of health service providers, that is prescribed by the regulations as an exempt health service provider—

(i) for the purposes of this Act generally, or

(ii) for the purposes of specified provisions of this Act, or

(iii) for the purposes of specified Health Privacy Principles or health privacy codes of practice, or

(iv) to the extent to which it is prescribed by the regulations as an exempt health service provider, or

(b) an organisation that merely arranges for a health service to be provided to an individual by another organisation.

healthcare identifier has the same meaning as it has in the *Healthcare Identifiers Act 2010* of the Commonwealth.

identifier means an identifier (which is usually, but need not be, a number), not being an identifier that consists only of the individual's name, that is—

(a) assigned to an individual in conjunction with or in relation to the individual's health information by an organisation for the purpose of uniquely identifying that individual, whether or not it is subsequently used otherwise than in conjunction with or in relation to health information, or

(b) adopted, used or disclosed in conjunction with or in relation to the individual's health information by an organisation for the purpose of uniquely identifying that individual.

immediate family member of an individual means a person who is—

(a) a parent, child or sibling of the individual, or

(b) a spouse of the individual, or

(c) a member of the individual's household who is a relative of the individual, or

(d) a person nominated to an organisation by the individual as a person to whom health information relating to the individual may be disclosed.

investigative agency means any of the following—

(a) the Ombudsman's Office,

(b) the Independent Commission Against Corruption,

(b1) the Inspector of the Independent Commission Against Corruption,

(c) the Law Enforcement Conduct Commission,

(d) the Inspector of the Law Enforcement Conduct Commission and any staff of the Inspector,

(e) the Community Services Commission,

(f) the Health Care Complaints Commission,

(g) the office of Legal Services Commissioner,

(g1) the Ageing and Disability Commissioner,

(g2) the Children's Guardian,

(h) a person or body prescribed by the regulations for the purposes of this definition.

law enforcement agency means any of the following—

(a) the NSW Police Force, or the police force of another State or a Territory,

(b) the New South Wales Crime Commission,

(c) the Australian Federal Police,

(d) the Australian Crime Commission,

(e) the Director of Public Prosecutions of New South Wales, of another State or a Territory or of the Commonwealth,

(f) the Department of Corrective Services,

(g) the Department of Juvenile Justice,

(h) a person or body prescribed by the regulations for the purposes of this definition.

local government authority means a council, a county council or a joint organisation within the meaning of the *Local Government Act 1993*.

news activity means—

(a) the gathering of news for the purposes of dissemination to the public or any section of the public, or

(b) the preparation or compiling of articles or programs of or concerning news, observations on news or current affairs for the purpose of dissemination to the public or any section of the public, or

(c) the dissemination to the public or any section of the public of any article or program of or concerning news, observations on news or current affairs.

news medium means any organisation whose business, or whose principal business, consists of a news activity.

organisation means a public sector agency or a private sector person.

personal information has the meaning given by section 5.

PPIP Act means the *Privacy and Personal Information Protection Act 1998*.

Privacy Commissioner means the Privacy Commissioner appointed under the PPIP Act.

private sector person means any of the following that is not a public sector agency—

(a) a natural person,

(b) a body corporate,

(c) a partnership,

(d) a trust or any other unincorporated association or body,

but does not include a small business operator within the meaning of the *Privacy Act 1988* of the Commonwealth, or an agency within the meaning of that Act.

Note—

Small business operator is defined in section 6D of the *Privacy Act 1988* of the Commonwealth. Several types of businesses or activities are excluded from that definition. In particular, under section 6D (4) (b) an individual, body corporate, partnership, unincorporated association or trust is not a small business operator if it provides a health service to an individual and holds any health information except in an employee record.

public sector agency means any of the following—

(a) a government department or the Teaching Service,

(b) a statutory body representing the Crown,

(c) (Repealed)

(d) an auditable entity within the meaning of the *Government Sector Audit Act 1983* or any other entity within the meaning of that Act (or entity of a kind) prescribed by the regulations, but excluding an entity (or entity of a kind) prescribed by the regulations,

(e) the NSW Police Force,

(e1) Service NSW Division of the Government Service,

(f) a local government authority,

(g) a person or body that—

(i) provides data services (being services relating to the collection, processing, disclosure or use of personal information or that provide for access to such information) for or on behalf of a body referred to in paragraphs (a)–(f), or that receives funding from any such body in connection with providing data services, and

(ii) is prescribed by the regulations for the purposes of this definition,

but does not include a State owned corporation.

public sector official means any of the following—

(a) a person appointed by the Governor, or a Minister, to a statutory office,

(b) a judicial officer within the meaning of the *Judicial Officers Act 1986*,

(c) a person employed in the Government Service, the Teaching Service, the NSW Health Service or the NSW Police Force,

(d) a local government councillor or a person employed by a local government authority,

(e) a person who is an officer of the Legislative Council or Legislative Assembly or who is employed by (or who is under the control of) the President of the Legislative Council or the Speaker of the Legislative Assembly, or both,

(f) a person who is employed or engaged by—

(i) a public sector agency, or

(ii) a person referred to in paragraphs (a)–(e),

(g) a person who acts for or on behalf of, or in the place of, or as deputy or delegate of, a public sector agency or person referred to in paragraphs (a)–(e).

related body corporate, in relation to an organisation that is a body corporate, has the same meaning as in the *Corporations Act 2001* of the Commonwealth.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother or step-sister of the individual.

spouse means—

(a) the person to whom a person is legally married (including the husband or wife of a person), or

(b) a de facto partner,

but where more than one person would so qualify as a spouse, means only the last person so to qualify.

Note—

"De facto partner" is defined in section 21C of the *Interpretation Act 1987*.

staff of the Inspector of the Independent Commission Against Corruption means—

(a) any staff employed under section 57E (1) or (2) of the *Independent Commission Against Corruption Act 1988*, and

(b) any consultants engaged under section 57E (3) of that Act.

staff of the Inspector of the Law Enforcement Conduct Commission means the staff of the Inspector within the meaning of section 128 (1) of the *Law Enforcement Conduct Commission Act 2016*.

stage, of an emergency, means a stage in relation to an emergency mentioned in the *State Emergency and Rescue Management Act 1989*, section 5.

State record has the same meaning as in the *State Records Act 1998*.

Tribunal means the Civil and Administrative Tribunal.

Note—

The *Interpretation Act 1987* contains definitions and other provisions that affect the interpretation and application of this Act.

(2) A reference in this Act to non-compliance with a requirement of this Act being permitted (or necessarily implied or reasonably contemplated) under an Act or other law includes a reference to non-compliance that is permitted (or necessarily implied or reasonably contemplated) under an Act of the Commonwealth.

(3) Notes included in this Act do not form part of this Act.

5 Definition of "personal information"

(1) In this Act, ***personal information*** means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

(2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

(3) Personal information does not include any of the following—

(a) information about an individual who has been dead for more than 30 years,

(b) information about an individual that is contained in a generally available publication,

(c) information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition,

(d) information about an individual that is contained in a State record under the control of the State Records Authority that is available for public inspection in accordance with the *State Records Act 1998*,

(e) information about an individual that is contained in archives within the meaning of the *Copyright Act 1968* of the Commonwealth,

(f) information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act,

(g) information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth,

(h) information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 1994*, or that has been collected in the course of an investigation arising out of a public interest disclosure,

(i) information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*,

(j) information about an individual arising out of a Royal Commission or Special Commission of Inquiry,

(k) information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*,

(l) information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*,

(m) information or an opinion about an individual's suitability for appointment or employment as a public sector official,

(n) information about an individual that forms part of an employee record (within the meaning of the *Privacy Act 1988* of the Commonwealth) about the individual held by a private sector person,

(o) information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

6 Definition of "health information"

In this Act, ***health information*** means—

(a) personal information that is information or an opinion about—

(i) the physical or mental health or a disability (at any time) of an individual, or

(ii) an individual's express wishes about the future provision of health services to him or her, or

(iii) a health service provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or

(e) healthcare identifiers,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

7 Capacity

(1) An individual is incapable of doing an act authorised, permitted or required by this Act if the individual is incapable (despite the provision of reasonable assistance by another person) by reason of age, injury, illness, physical or mental impairment of—

(a) understanding the general nature and effect of the act, or

(b) communicating the individual's intentions with respect to the act.

(2) An authorised representative of an individual may do such an act on behalf of an individual who is incapable of doing that act.

(3) An authorised representative may not do such an act on behalf of an individual who is capable of doing that act, unless the individual expressly authorises the authorised representative to do that act.

8 Definition of "authorised representative"

(1) In this Act, ***authorised representative***, in relation to an individual, means—

(a) an attorney for the individual under an enduring power of attorney, or

(b) a guardian within the meaning of the *Guardianship Act 1987*, or a person responsible within the meaning of Part 5 of that Act, or

(c) a person having parental responsibility for the individual, if the individual is a child, or

(d) a person who is otherwise empowered under law to exercise any functions as an agent of or in the best interests of the individual.

(2) A person is not an authorised representative of an individual for the purposes of this Act to the extent that acting as an authorised representative of the individual is inconsistent with an order made by a court or tribunal.

(3) In this section—

child means an individual under 18 years of age.

parental responsibility, in relation to a child, means all the duties, powers, responsibility and authority which, by law, parents have in relation to their children.

9 What constitutes "holding" information

For the purposes of this Act, health information is ***held*** by an organisation if—

(a) the organisation is in possession or control of the information (whether or not the information is contained in a document that is outside New South Wales), or

(b) the information is in the possession or control of a person employed or engaged by the organisation in the course of such employment or engagement, or

(c) in the case of a public sector agency—the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

10 Unsolicited information not considered "collected"

For the purposes of this Act, health information is not collected by an organisation if the receipt of the information by the organisation is unsolicited.

Part 2 General operation of Act

11 How this Act applies to organisations

(1) This Act applies to every organisation that is a health service provider or that collects, holds or uses health information.

Note—

The term ***organisation*** means a public sector agency or a private sector person.

(2) An organisation to whom or to which this Act applies is required to comply with the Health Privacy Principles and with any health privacy code of practice or provision of Part 4 that is applicable to the organisation.

(3) An organisation must not do any thing, or engage in any practice, that contravenes a Health Privacy Principle or a health privacy code of practice or a provision of Part 4 in respect of which the organisation is required to comply.

Note—

The application of Health Privacy Principles and the provisions of Part 4 may be modified by health privacy codes

of practice. See section 39.

12 Crown bound by Act

This Act binds the Crown in right of New South Wales and also, in so far as the legislative power of Parliament permits, the Crown in all its other capacities.

13 Courts, tribunals and Royal Commissions not affected

(1) Nothing in this Act affects the manner in which a court or tribunal, or the manner in which the holder of an office relating to a court or tribunal, exercises the court's, or the tribunal's, judicial functions.

(2) Nothing in this Act affects the manner in which a Royal Commission, or any Special Commission of Inquiry, exercises the Commission's functions.

(3) In this section, ***judicial functions of a court or tribunal*** means such of the functions of the court or tribunal as relate to the hearing or determination of proceedings before it, and includes—

(a) in relation to a justice—such of the functions of the justice as relate to the conduct of committal proceedings, and

(b) in relation to a coroner—such of the functions of the coroner as relate to the conduct of inquests and inquiries under the *Coroners Act 2009*.

14 Exemption for personal, family or household affairs

Nothing in this Act applies in respect of the collection, holding, management, use, disclosure or transfer of health information by an individual, or health information held by an individual, only for the purposes of, or in connection with, his or her personal, family or household affairs.

15 News media

(1) Nothing in HPP 1–4, 10, 11 or 14 applies in respect of the collection, use or disclosure of health information by a news medium if the collection, use or disclosure is in connection with its news activities.

(2) Nothing in HPP 6–8 or Part 4 applies to health information held by a news medium in connection with its news activities.

16 Group practices

(1) Nothing in HPP 1–6, 10 or 11 applies in respect of—

(a) the collection of information from a member of a group practice by another member of the group practice, or

(b) the use of health information held by a member of a group practice by another

member of the group practice, or

(c) the disclosure of health information held by a member of a group practice to another member of the group practice,

if the purpose of the collection, use or disclosure is to ensure that a patient of a member of the group practice receives quality health care from members of the group practice.

(2) Nothing in HPP 15 applies in respect of the keeping of combined or joint electronic records by members of a group practice.

(3) In this section—

group practice means—

(a) a group of 2 or more individuals who each provide a health service in the course of carrying on a business and who, by written agreement—

(i) carry on the business at shared premises, and

(ii) maintain a shared reception, and

(iii) maintain combined or joint records, or

(b) the provision of a health service in accordance with such other arrangements or associations between health service providers as may be prescribed by the regulations for the purposes of this definition.

17 Specific exemptions (ICAC, ICAC Inspector and Inspector's staff, NSW Police Force, LECC, Inspector of LECC and Inspector's staff and NSW Crime Commission)

This Act does not apply to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, the NSW Police Force, the Law Enforcement Conduct Commission, the Inspector of the Law Enforcement Conduct Commission, the staff of the Inspector of the Law Enforcement Conduct Commission and the New South Wales Crime Commission, except in connection with the exercise of their administrative and educative functions.

17A Exemption for certain translation services

The Health Privacy Principles do not apply in respect of health information collected or held by Multicultural NSW if—

(a) the information is collected or held by Multicultural NSW for the purpose only of translating the information, and

(b) all documents held by Multicultural NSW in which the information is contained are

destroyed or returned to the person who submitted the information for translation when Multicultural NSW is satisfied that the documents are no longer required for the provision of the translation service, and

(c) in a case where it is necessary for the information to be given to another person in connection with the provision of the translation service, everything reasonably within the power of Multicultural NSW is done to prevent unauthorised disclosure of the information by that other person.

18 Act does not authorise unauthorised activities

If an organisation is exempt from a Health Privacy Principle, or a provision of Part 4, the exemption does not operate to authorise the organisation to do any thing that it is otherwise prohibited from doing under an Act (including an Act of the Commonwealth) or any other law.

19 Application of Health Privacy Principles to information collected at certain times

(1) Except as otherwise provided by this section, the Health Privacy Principles apply in relation to all health information, whether collected by the organisation before or after the commencement of Schedule 1.

(2) HPP 1 (Purposes of collection of health information), HPP 2 (Information must be relevant, not excessive, accurate and not intrusive), HPP 3 (Collection to be from individual concerned) and HPP 4 (Individual to be made aware of certain matters), to the extent that they apply to the collection of health information, apply only in relation to the collection of health information after the commencement of Schedule 1.

(3) HPP 7 (Access to health information), HPP 8 (Amendment of health information) and Divisions 3 and 4 of Part 4 apply to all health information collected after the commencement of Schedule 1 and also apply to the following health information collected before that commencement—

(a) a history of the health or an illness of an individual,

(b) any findings on an examination of the individual in relation to the health or an illness of an individual,

(c) the results of an investigation into the health or an illness of an individual,

(d) a diagnosis, or preliminary diagnosis, of an illness of an individual,

(e) a plan of management, or proposed plan of management, of the treatment or care of an illness of the individual,

(f) action taken or services provided (whether or not in accordance with a plan of management) by or under the direction or referral of a health service provider in relation to the individual,

(g) health information about the individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances,

(h) genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual.

(4) HPP 13 (Anonymity) applies only in relation to transactions entered into, or health services received, after the commencement of Schedule 1.

(5) HPP 15 (Linkage of health records) applies only in relation to information collected after the commencement of Schedule 1.

Part 3 Provisions for public sector agencies

Note—

Section 11 requires organisations to which this Act applies (including public sector agencies) to comply with the Health Privacy Principles. This Part makes special provision for public sector agencies, while Part 4 makes special provision for private sector persons.

20 Application of Health Privacy Principles—amendment of health information

HPP 8 (Amendment of health information), and any provision of a health privacy code of practice applying to a public sector agency that relates to the requirements set out in that Health Privacy Principle, applies to public sector agencies despite HPP 8 (4) and section 21 of the *State Records Act 1998*.

21 Complaints against public sector agencies

(1) The following conduct by a public sector agency is conduct to which Part 5 (Review of certain conduct) of the PPIP Act applies—

(a) the contravention of a Health Privacy Principle that applies to the agency,

(b) the contravention of a health privacy code of practice that applies to the agency.

(2) For that purpose, a reference in that Part—

(a) to personal information is taken to include health information, and

(b) to an information protection principle is taken to include a Health Privacy Principle, and

(c) to a privacy code of practice is taken to include a health privacy code of practice.

(3) This section applies only to conduct engaged in after the commencement of this section.

22 Government Information (Public Access) Act 2009 not affected

(1) Nothing in this Act affects the operation of the *Government Information (Public Access) Act 2009*.

(2) In particular, this Act does not operate to lessen any obligations under the *Government Information (Public Access) Act 2009* in respect of a public sector agency.

(3) Without limiting the generality of subsection (1), the provisions of the *Government Information (Public Access) Act 2009* and the *Privacy and Personal Information Protection Act 1998* that impose conditions or limitations (however expressed) with respect to any matter referred to in HPP 6 (Information about health information held by organisations), HPP 7 (Access to health information) or HPP 8 (Amendment of health information) are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.

Part 4 Provisions for private sector persons

Note—

Section 11 requires organisations to which this Act applies (including private sector persons) to comply with the Health Privacy Principles and the provisions of this Part. This Part makes special provision for private sector persons, while Part 3 makes special provision for public sector agencies.

Division 1 General

23 When non-compliance authorised

A private sector person is not required to comply with a requirement of this Part applying to the person if—

(a) the private sector person is lawfully authorised or required not to comply with it, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law.

24 Guidelines by Privacy Commissioner

The Privacy Commissioner may issue guidelines with respect to access to, and retention and amendment of, health information held by private sector persons for the purpose of assisting them to comply with the Health Privacy Principles and this Part.

Division 2 Retention of health information

Note—

This Division contains specific provisions that are additional to, and assist the operation of, the general principles in HPP 5 (Retention and security).

25 Retention of health information: health service providers

(1) A private sector person who is a health service provider must retain health information relating to an individual as follows—

(a) in the case of health information collected while the individual was an adult—for 7 years from the last occasion on which a health service was provided to the individual by the health service provider,

(b) in the case of health information collected while the individual was under the age of 18 years—until the individual has attained the age of 25 years.

(2) A health service provider who deletes or disposes of health information must keep a record of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted or disposed of.

(3) A health service provider who transfers health information to another organisation and does not continue to hold a record of that information must keep a record of the name and address of the organisation to whom or to which it was transferred.

(4) A record referred to in subsection (2) or (3) may be kept in electronic form, but only if it is capable of being printed on paper.

(5) Nothing in this section authorises a health service provider to delete, dispose of or transfer health information in contravention of an Act (including an Act of the Commonwealth) or any other law.

Division 3 Access to health information

Note—

This Division contains specific provisions for private sector persons that are additional to, and assist the operation of, the general principles in HPP 7 (Access to health information).

26 Making a request for access

(1) An individual may request a private sector person to provide the individual with access to health information relating to the individual held by the private sector person. A request must—

(a) be in writing, and

(b) state the name and the address of the individual making the request, and

(c) sufficiently identify the health information to which access is sought, and

(d) specify the form in which the individual wishes the information to be provided, being a form provided for by this Act.

(2) An individual who requests access to health information relating to the individual may

authorise another person to have access to the information in the place of the individual. Such an authority must—

(a) be in writing, and

(b) name the person who is authorised to have access to the information.

A private sector person is to provide access under this Act in accordance with any such written authority.

Note—

This section does not prevent an individual and a private sector person from making other arrangements for access to information: see section 32.

27 Response to request for access

(1) A private sector person must respond to a request for access within 45 days after receiving the request.

(2) A private sector person responds to a request for access by—

(a) providing access to the information as required by this Act, or

(b) refusing access to the information.

(3) A private sector person who refuses to give an individual access to information must give the individual a written reason for refusal of access, being a reason for refusal provided for by this Act.

(4) A private sector person who charges a fee for providing access to information need not provide access until 7 days after payment of the fee, if—

(a) the private sector person has given the individual written notice stating that access will be provided on payment of a specified fee, and

(b) that notice is given within 45 days after receiving a request.

(5) Access may be refused to a part of the information to which a request relates (with access provided to the remainder of the information).

(6) A private sector person is taken to have refused access to health information if the private sector person fails to respond to the request for access as required by this section.

28 Form of access

(1) Access to health information relating to an individual is to be provided to the individual—

(a) by giving the individual a copy of the health information, or

(b) by giving the individual a reasonable opportunity to inspect and take notes from the health information.

(2) If an individual has requested that access to health information be provided in a particular form, the private sector person is to provide access in that form, and in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this section.

(3) Despite subsection (2), a private sector person may refuse to provide access to health information in the form requested if providing the information in that form—

(a) would place unreasonable demands on the organisation's resources, or

(b) would be detrimental to the preservation of the information or (having regard to the physical form in which the information is contained) would otherwise not be appropriate, or

(c) would involve an infringement of copyright subsisting in matter contained in the information.

If access is refused under this clause, the information is to be provided in another form.

(4) Despite anything to the contrary in this Part or HPP 7, a private sector person who receives a request for access to health information collected before the commencement of this section need only give the individual an accurate summary of the health information.

29 Situations where access need not be granted

A private sector person is not required to provide an individual with access to health information relating to the individual held by the private sector person if—

(a) providing access would pose a serious threat to the life or health of the individual or any other person and refusing access is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(b) providing access would have an unreasonable impact on the privacy of other individuals and refusing access is in accordance with guidelines, if any, issued by the Privacy Commissioner, or

(c) the information relates to existing or anticipated legal proceedings between the private sector person and the individual and the information would not be accessible by the process of discovery in those proceedings or is subject to legal professional privilege, or

(d) providing access would reveal the intentions of the private sector person in relation to negotiations, other than about the provision of a health service, with the individual in

such a way as to expose the private sector person unreasonably to disadvantage, or

(e) providing access would be unlawful, or

(f) denying access is required or authorised by or under law, or

(g) providing access would be likely to prejudice an investigation of possible unlawful activity, or

(h) providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency, or

(i) a law enforcement agency performing a lawful security function asks the private sector person not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia, or

(j) the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again, or

(k) the individual has been provided with access to the health information in accordance with this Act and is making an unreasonable, repeated request for access to the same information in the same manner.

30 Access refused because serious threat to individual

(1) This section applies if a private sector person that holds health information about an individual refuses to provide the individual with access to the health information on the ground that providing access would pose a serious threat to the life or health of the individual.

(2) The individual may request the private sector person to give access to the information to a registered medical practitioner nominated by the individual.

(3) The request is to be made within 21 days after the notice of refusal was received.

(4) The notice of refusal—

(a) must advise the individual that he or she may nominate a medical practitioner to be given access to the health information, and

(b) must advise the individual that if he or she nominates a medical practitioner, the nomination must be made to the private sector person within 21 days after receiving the notice of refusal.

(5) The private sector person must provide access to the health information to the nominated registered medical practitioner within 21 days after being advised by the individual of the nomination of the practitioner.

31 Private sector person may require evidence of identity or authority

(1) Before a private sector person provides access to health information to a person, the private sector person must take reasonable steps to be satisfied about that person's authority to have access to the information.

(2) For this purpose, the private sector person may require evidence of—

(a) the person's identity, and

(b) if person seeking access claims to be authorised to have access to the information under section 26 (2), the authority of that person, and

(c) if the person seeking access claims to be an authorised representative of the individual to whom the information relates, the authority of that person.

Note—

The term ***authorised representative*** is defined in section 8.

32 Alternative arrangements may be made

(1) Nothing in this Division is intended to prevent or discourage a private sector person from providing an individual, with his or her consent, with access to his or her health information otherwise than as required by this Division.

(2) A private sector person is not to provide an individual with access to health information otherwise than as required by this Division unless the private sector person has informed the individual of the requirements of this Division.

Division 4 Amendment of health information

Note—

This Division contains specific provisions for private sector persons that are additional to, and assist the operation of, the general principles in HPP 8 (Amendment of health information).

33 Making a request for amendment

An individual may request a private sector person to amend health information relating to the individual held by the private sector person. The request must—

(a) be in writing, and

(b) state the name and the address of the individual making the request, and

(c) identify the health information concerned, and

(d) specify the respect or respects in which the individual claims the health information is inaccurate, out of date, irrelevant, incomplete or misleading, and

(e) if the request specifies that the individual claims the health information is incomplete or out of date—be accompanied by such information as the individual claims is necessary to complete the health information or to bring it up to date.

34 Response to request for amendment

(1) A private sector person must respond to a request for amendment within 45 days after receiving the request.

(2) A private sector person responds to a request by—

(a) making the amendment requested, or

(b) refusing to make the amendment requested.

(3) A private sector person may refuse to amend health information in accordance with a request—

(a) if it is satisfied that the health information is not incomplete, incorrect, irrelevant, out of date or misleading, or

(b) if it is satisfied that the request contains or is accompanied by matter that is incorrect or misleading in a material respect.

(4) A private sector person who refuses to make an amendment requested must give the individual a written reason for the refusal.

(5) A private sector person is taken to have refused to make the amendment requested if the private sector person fails to respond to the request for amendment as required by this section.

35 Notations added to records

(1) If a private sector person has refused to amend health information held by the person, the individual to whom the information relates may, by notice in writing, require the private sector person to add to the health information a notation—

(a) specifying the respects in which the individual claims the information to be incomplete, incorrect, irrelevant, out of date or misleading, and

(b) if the individual claims the information to be incomplete or out of date—setting out such information as the individual claims is necessary to complete the information or to bring it up to date.

(2) The private sector person must take reasonable steps to comply with the requirements of a notice given under this section and is to cause written notice of the steps taken, and the nature of a notation, to be given to the individual.

(3) If the private sector person discloses to any person or organisation (including any

public sector agency or any Minister) any health information to which a notice under this section relates, the private sector person—

(a) must ensure that there is given to that person or organisation, when the information is disclosed, a statement—

(i) stating that the person to whom the information relates claims that the information is incomplete, incorrect, irrelevant, out of date or misleading, and

(ii) setting out particulars of a notation added to the information under this section, and

(b) may include in the statement the reason for the private sector person's refusal to amend its records in accordance with the notation.

(4) Nothing in this section is intended to prevent or discourage private sector persons from giving particulars of a notation added to health information under this section to a person or organisation (including a public sector agency or any Minister) to whom information was given before the commencement of this section.

36 Private sector person may require evidence of identity or authority

(1) Before a private sector person amends health information at the request of an individual or an authorised representative of the individual, the private sector person must take reasonable steps to be satisfied about the authority of the person making the request to request amendment of the information.

(2) For this purpose, the private sector person may require evidence of—

(a) the identity of the person making the request, and

(b) if the person making the request claims to be an authorised representative of the individual to whom the information relates, the authority of that person.

Note—

The term ***authorised representative*** is defined in section 8.

37 Alternative arrangements may be made

(1) Nothing in this Division is intended to prevent or discourage a private sector person from providing an individual, with his or her consent, with an opportunity to amend his or her health information otherwise than as required by this Division.

(2) A private sector person is not to provide an individual with an opportunity to amend health information otherwise than as required by this Division unless the private sector person has informed the individual of the requirements of this Division.

Part 5 Health privacy codes of practice

38 Operation of health privacy codes of practice

(1) Health privacy codes of practice may be made for the purpose of protecting the privacy of health information with respect to individuals.

(2) A health privacy code of practice may regulate any of the following matters—

(a) the collection or retention of health information held by organisations,

(b) the use or disclosure of health information held by organisations,

(c) the transfer by organisations of health information from New South Wales to a jurisdiction outside New South Wales or to a Commonwealth agency,

(d) the electronic or computerised linkage of health information held by organisations,

(e) the procedures for dealing with health information held by organisations.

(3) In particular, a health privacy code of practice may provide for the protection of health information contained in a record that is more than 30 years old, and any such provision has effect despite the provisions of any other Act that deals with the disclosure of, or access to, health information of that kind. Any such code must, to the extent that it relates to health information contained in a State record that is more than 30 years old, be consistent with any relevant guidelines issued under section 52 of the *State Records Act 1998*.

(4) A health privacy code of practice can apply to any one or more of the following—

(a) any specified class of health information,

(b) any specified organisation or class of organisation,

(c) any specified activity or class of activity.

(5) Except in the case of a health privacy code of practice that is referred to in subsection (3), a code cannot affect the operation of any exemption provided under this Act.

(6) A health privacy code of practice—

(a) must provide standards of health information privacy protection that operate to protect organisations from any restrictions in relation to the importation of health information into New South Wales, and

(b) must not impose on any organisation any requirements that are more stringent (or of a higher standard) than the Health Privacy Principles.

39 Modification of Health Privacy Principles or Part 4

(1) A health privacy code of practice may modify the application to any organisation or class of organisation of any one or more of the Health Privacy Principles or any provision of Part 4.

(2) A code may—

(a) specify requirements that are different from the requirements set out in the Health Privacy Principles or in a provision of Part 4, or exempt any activity or conduct of or by the organisation or class of organisation from compliance with any such Principle or provision, or

(b) specify the manner in which any one or more of the Health Privacy Principles or any provision of Part 4 are to be applied to, or are to be followed by, the organisation or class of organisation, and

(c) exempt an organisation or class of organisation from the requirement to comply with any Health Privacy Principle or any provision of Part 4.

40 Preparation and making of health privacy codes of practice

(1) The Privacy Commissioner, or any organisation, may—

(a) initiate the preparation of a draft health privacy code of practice, and

(b) develop the draft code in consultation with such other persons or bodies as the Commissioner or organisation thinks fit, and

(c) submit the draft code to the Minister.

(2) If a draft code is initiated and prepared by an organisation, the organisation must consult with the Privacy Commissioner on the draft code before it is submitted to the Minister.

(3) The Privacy Commissioner may make such submissions to the Minister in respect of a draft code as the Privacy Commissioner thinks appropriate.

(4) Once a draft code is submitted to the Minister, the Minister may, after taking into consideration any submissions by the Privacy Commissioner and after consulting the Attorney General, and Minister for the Prevention of Domestic Violence about the draft code, decide to make the code.

(5) A health privacy code of practice is made by order of the Minister published in the Gazette.

(6) A code takes effect when the order making the code is published (or on such later date as may be specified in the order).

(7) The procedures specified in this section extend to any amendment of a health privacy code of practice.

Part 6 Complaints against private sector persons

Division 1 General

41 Definitions

In this Part—

complainant, in relation to a complaint, means the person who makes the complaint.

respondent, in relation to a complaint, means a person against whom the complaint is made.

42 Making of privacy related complaints

(1) A complaint may be made to the Privacy Commissioner about the alleged contravention of any of the following by a private sector person—

(a) a Health Privacy Principle,

(b) a provision of Part 4,

(c) a health privacy code of practice.

(2) A complaint must be made—

(a) in writing, and

(b) in accordance with such regulations (if any) as may be made for the purposes of this section.

(3) A complaint must be made within 6 months (or such later time as the Privacy Commissioner may allow) after the time the complainant first became aware of the conduct the subject of the complaint.

(4) A complainant may amend or withdraw a complaint.

(5) This Part does not apply to any conduct that occurred before the commencement of this Part.

43 Preliminary assessment of complaints

(1) The Privacy Commissioner may conduct a preliminary assessment of a complaint made under this Part for the purpose of deciding whether to deal with the complaint.

(2) The Privacy Commissioner may decide not to deal with a complaint if the Privacy Commissioner is satisfied that—

(a) the complaint is frivolous, vexatious or lacking in substance, or is not in good faith, or

(b) the subject matter of the complaint is trivial, or

(c) the subject matter of the complaint relates to a matter permitted or required by or under any law, or

(d) there is available to the complainant an alternative, satisfactory and readily available means of redress, or

(e) the matter should be referred to the Health Care Complaints Commission or another person or body under section 65, 66 or 67, or

(f) the person has made a complaint about the same subject matter to the Commonwealth Privacy Commissioner, or to an adjudicator under an approved privacy code within the meaning of the *Privacy Act 1988* of the Commonwealth, and—

(i) the complaint has not been withdrawn, or

(ii) the Commonwealth Privacy Commissioner has made a determination under section 52 of that Act, or

(iii) the adjudicator has made a determination under a provision of the approved privacy code that corresponds to section 52 of that Act.

(3) If the Privacy Commissioner decides not to deal with a complaint, the Privacy Commissioner must advise the complainant of the reasons for deciding not to deal with the complaint.

44 Assessment of complaints

(1) If the Privacy Commissioner decides to deal with a complaint made under this Part, the Privacy Commissioner—

(a) is to carry out an assessment to determine whether there is a prima facie case that the respondent contravened a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice, and

(b) for that purpose, may make such inquiries and investigations into the complaint as the Privacy Commissioner thinks appropriate.

(2) If, after carrying out such an assessment, the Privacy Commissioner is satisfied that there is no prima facie case that the respondent contravened a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice, the Privacy Commissioner is to cease to deal with the complaint.

(3) If the Privacy Commissioner ceases to deal with a complaint, the Privacy

Commissioner must advise the complainant of the reasons for ceasing to deal with the complaint.

45 Dealing with complaint

(1) If the Privacy Commissioner is satisfied that there is a prima facie case that the respondent contravened a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice, the Privacy Commissioner may—

(a) endeavour to resolve the complaint by conciliation under section 46, or

(b) further investigate the complaint and make a report under section 47, or

(c) determine that the complaint has been resolved to his or her satisfaction.

(2) In deciding which course of action to take, the Privacy Commissioner is to take into consideration the following matters—

(a) the nature of the complaint,

(b) the views of the complainant and respondent,

(c) any action taken by the respondent (or that the respondent gives an undertaking to take) to address the complaint,

(d) whether the complaint raises a matter of public interest.

(3) If the Privacy Commissioner determines that the complaint has been resolved to his or her satisfaction under subsection (1) (c), the Privacy Commissioner is to—

(a) notify the complainant and the respondent of the determination, and

(b) take no further action on the complaint.

46 Resolution of complaint by conciliation

(1) The Privacy Commissioner may endeavour to resolve the complaint by conciliation.

(2) The Privacy Commissioner may by written notice request the complainant and the respondent to appear before the Privacy Commissioner in conciliation proceedings.

(3) A person or body must not without reasonable excuse fail to comply with the terms of a notice under subsection (2).

Maximum penalty—50 penalty units in the case of a body corporate or 10 penalty units in any other case.

(4) The parties to any such conciliation proceedings before the Privacy Commissioner are not entitled to be represented by any other person except by leave of the Privacy Commissioner.

(5) The procedures for conciliation are to be determined by the Privacy Commissioner.

(6) Evidence of anything said or done in the course of conciliation proceedings under this section is not admissible in subsequent proceedings under this Part relating to the complaint.

(7) The Privacy Commissioner is to take no further action after the conclusion of the conciliation proceedings, whether or not the parties reach any agreement as a result of the proceedings.

47 Reports and recommendations of Privacy Commissioner

(1) The Privacy Commissioner may make a written report as to any findings or recommendations by the Privacy Commissioner in relation to a complaint dealt with by the Privacy Commissioner under section 45 (1) (b).

(2) The Privacy Commissioner may give a copy of any such report to the complainant, the respondent and to such other persons or bodies as appear to be materially involved in matters concerning the complaint.

(3) A report under this section is admissible in subsequent proceedings under this Part relating to the complaint.

Division 2 Functions of the Tribunal

Note—

The *Civil and Administrative Tribunal Act 2013* contains provisions dealing with the practice and procedure of the Tribunal, including matters concerning parties and their representation.

48 Application to Tribunal

(1) A person who has made a complaint to the Privacy Commissioner under Division 1 may apply to the Tribunal for an inquiry into the complaint, but only if the complaint was the subject of a report of the Privacy Commissioner under section 47.

Note—

This section confers jurisdiction on the Tribunal to make an original decision. It does not confer jurisdiction to review a decision of the Privacy Commissioner.

(2) An application may only be made within 28 days after—

(a) the day on which the complainant received the report of the Privacy Commissioner, or

(b) the day (if any) recommended in the report of the Privacy Commissioner as the day after which an application may be made to the Tribunal,

whichever is later.

(3) However, a person cannot apply to the Tribunal if the person has made a complaint about the same subject matter to the Commonwealth Privacy Commissioner, or to an adjudicator under an approved privacy code within the meaning of the *Privacy Act 1988* of the Commonwealth, and—

(a) the complaint has not been withdrawn, or

(b) the Commonwealth Privacy Commissioner has made a determination under section 52 of that Act, or

(c) the adjudicator has made a determination under a provision of the approved privacy code that corresponds to section 52 of that Act.

49 Inquiries into complaints

The Tribunal is to hold an inquiry into a complaint that is the subject of an application.

50 Appearance by Privacy Commissioner

(1) The Privacy Commissioner is to be notified by the Tribunal of any application made to it under section 48.

(2) The Privacy Commissioner has a right to appear and be heard in any proceedings before the Tribunal in relation to an inquiry under this Part.

51 Proof of exemption

If in proceedings in relation to an inquiry into a complaint the respondent relies on an exemption under any provision of this Act or the regulations, the onus of proving that the exemption applies to the respondent in the circumstances lies on the respondent.

52 Tribunal may dismiss frivolous etc complaints

(1) If, at any stage of an inquiry into a complaint, the Tribunal is satisfied that the complaint is frivolous, vexatious, misconceived or lacking in substance, or that for any other reason the complaint should not be dealt with, it may dismiss the complaint.

(2) The Tribunal may dismiss a complaint if satisfied that the person does not wish to proceed with the complaint.

(3) If the Tribunal dismisses a complaint under this section, it may order the complainant to pay the costs of the inquiry.

53 Relationship to Civil and Administrative Tribunal Act 2013

Nothing in section 52 limits the generality of the powers conferred on the Tribunal by Part 4 of the *Civil and Administrative Tribunal Act 2013*.

54 Order or other decision of Tribunal

(1) After holding an inquiry, the Tribunal may decide not to take any action on the matter, or it may make any one or more of the following orders—

(a) subject to subsection (2), an order requiring the respondent to pay to the complainant damages not exceeding $40,000 if the respondent is a body corporate, or not exceeding $10,000 in any other case, by way of compensation for any loss or damage suffered by reason of the respondent's conduct,

(b) an order requiring the respondent to refrain from any conduct or action in contravention of a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice,

(c) an order requiring the performance of a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice,

(d) an order requiring health information that has been disclosed to be corrected by the respondent,

(e) an order requiring the respondent to take specified steps to remedy any loss or damage suffered by the complainant,

(f) such ancillary orders as the Tribunal thinks appropriate.

(2) The Tribunal may make an order under subsection (1) (a) only if—

(a) the application relates to conduct that occurs after the end of the 12-month period following the date on which Schedule 1 commences, and

(b) the Tribunal is satisfied that the applicant has suffered financial loss, or psychological or physical harm, because of the conduct of the respondent.

(3) In making an order for damages under this section concerning a complaint lodged on behalf of a person or persons, the Tribunal may make such order as it thinks fit as to the application of those damages for the benefit of the person or persons.

55–57 (Repealed)

Part 7 Privacy Commissioner

58 Functions of Privacy Commissioner

The Privacy Commissioner has the following functions—

(a) to promote the adoption of, and monitor compliance with, the Health Privacy Principles and the provisions of Part 4,

(b) to prepare and publish guidelines relating to the protection of health information and

other privacy matters, and to promote the adoption of such guidelines,

(c) to provide assistance to organisations in adopting and complying with the Health Privacy Principles and the provisions of Part 4,

(d) to conduct research, and collect and collate information, about any matter relating to the protection of health information and the privacy of individuals,

(e) to provide advice on matters relating to the protection of health information and the privacy of individuals,

(f) to receive, investigate and conciliate complaints about alleged contraventions of the Health Privacy Principles, the provisions of Part 4 or any health privacy code of practice,

(g) such other functions as are conferred by this Act.

Note—

The Privacy Commissioner may also deal with privacy related complaints under Parts 4 and 5 of the PPIP Act.

59 Requirement to give information

(1) The Privacy Commissioner may, in connection with the exercise of the Privacy Commissioner's functions, require any person or organisation—

(a) to give the Privacy Commissioner a statement of information, or

(b) to produce to the Privacy Commissioner any document or other thing, or

(c) to give the Privacy Commissioner a copy of any document.

(2) The Privacy Commissioner is not to make any such requirement if it appears to the Privacy Commissioner that—

(a) the person or organisation concerned does not consent to compliance with the requirement, and

(b) the person or organisation would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege.

(3) A requirement under this section must be in writing, must specify or describe the information, document or thing required, and must specify the time and manner for complying with the requirement.

(4) This section does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption.

60 Inquiries and investigations

(1) For the purposes of any inquiry or investigation conducted by the Privacy Commissioner under this Act, the Privacy Commissioner has the powers, authorities, protections and immunities conferred on a commissioner by Division 1 of Part 2 of the *Royal Commissions Act 1923*, and that Act (section 13 and Division 2 of Part 2 excepted) applies (subject to this section) to any witness summoned by or appearing before the Privacy Commissioner in the same way as it applies to a witness summoned by or appearing before a commissioner.

(2) Subsection (1) does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, Law Enforcement Conduct Commission, Inspector of the Law Enforcement Conduct, staff of the Inspector of the Law Enforcement Conduct Commission or New South Wales Crime Commission.

(3) Any inquiry or investigation conducted by the Privacy Commissioner under this Act is to be conducted in the absence of the public, except as otherwise directed by the Privacy Commissioner.

(4) The Privacy Commissioner, in the course of conducting an inquiry or investigation under this Act, must set aside any requirement—

(a) to give any statement of information, or

(b) to produce any document or other thing, or

(c) to give a copy of any document, or

(d) to answer any question,

if it appears to the Privacy Commissioner that the person or organisation concerned does not consent to compliance with the requirement and the person or organisation would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege. However, the person or organisation must comply with any such requirement despite any duty of secrecy or other restriction on disclosure.

(5) A person is not entitled to be represented by another person at an inquiry or investigation conducted by the Privacy Commissioner except with the leave of the Privacy Commissioner.

(6) The Privacy Commissioner may allow any person appearing before the Privacy Commissioner to have the services of an interpreter.

61 General procedure for inquiries and investigations

The Privacy Commissioner—

(a) may determine the procedures to be followed in exercising the Privacy Commissioner's functions under this Act, including the procedures to be followed at an inquiry or investigation conducted by the Privacy Commissioner, and

(b) is to act in an informal manner (including avoiding conducting formal hearings) as far as possible, and

(c) is not bound by the rules of evidence and may inform himself or herself on any matter in any way that the Privacy Commissioner considers to be just, and

(d) is to act according to the substantial merits of the case without undue regard to technicalities.

62 Exempting organisations from complying with Principles and codes

(1) The Privacy Commissioner may, in accordance with this section, make a written direction that—

(a) an organisation is not required to comply with a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice, or

(b) the application of a Health Privacy Principle, a provision of Part 4 or a code to an organisation is to be modified as specified in the direction.

(2) Any such direction has effect despite any other provision of this Act.

(3) The Privacy Commissioner is not to make a direction under this section unless—

(a) the Privacy Commissioner is satisfied that the public interest in requiring the organisation to comply with the Health Privacy Principle, the provision of Part 4 or health privacy code of practice is outweighed by the public interest in the Privacy Commissioner making the direction, and

(b) the Privacy Commissioner has consulted the Attorney General, and Minister for the Prevention of Domestic Violence about the direction, and

(c) the Minister has approved the making of the direction.

63 Information about compliance arrangements

(1) The Privacy Commissioner may require an organisation to provide the Commissioner with information—

(a) concerning the arrangements made by the organisation to enable the organisation to comply with the Health Privacy Principles, the provisions of Part 4 and any health privacy code of practice applying to the organisation, and

(b) demonstrating the means by which the organisation is implementing such arrangements.

(2) Any such requirement must be in writing and specify a time for complying with the requirement.

(3) This section does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, Law Enforcement Conduct Commission, Inspector of the Law Enforcement Conduct Commission, staff of the Inspector of the Law Enforcement Conduct Commission, New South Wales Crime Commission or Ombudsman's Office.

64 Guidelines by Privacy Commissioner

(1) The Privacy Commissioner may issue guidelines for or with respect to any matter for which guidelines may be issued under this Act. The Privacy Commissioner may from time to time amend or replace the guidelines.

(2) Guidelines issued by the Privacy Commissioner may apply, adopt or incorporate any publication as in force for the time being.

(3) The Minister may request the Privacy Commissioner to develop guidelines relating to any matter that the Minister considers should be the subject of guidelines.

(4) The procedure for the issuing of guidelines is as follows—

(a) the Privacy Commissioner is to prepare proposed guidelines in draft form and is to prepare an impact assessment statement for the proposed guidelines in accordance with such requirements as the Minister may from time to time determine,

(b) the draft guidelines and impact assessment statement are to be publicly exhibited for a period of at least 21 days,

(c) the Privacy Commissioner is to seek public comment on the draft guidelines during the period of public exhibition and public comment may be made during the period of the exhibition and for 21 days (or such longer period as the Privacy Commissioner may determine) after the end of that period,

(d) the Privacy Commissioner is to submit the draft guidelines to the Minister for approval together with a report by the Privacy Commissioner giving details of public comment received during the period allowed for public comment and the Privacy Commissioner's response to it,

(e) the Privacy Commissioner is not to issue the draft guidelines as guidelines unless

the Minister approves the guidelines.

(5) The procedure for the amendment or replacement of guidelines is the same as for the issuing of the guidelines unless the Minister otherwise directs in respect of a particular amendment.

65 Referring privacy related complaint to Health Care Complaints Commission

(1) The Privacy Commissioner may refer a complaint made under this Act to the Health Care Complaints Commission if the complaint concerns—

(a) the professional conduct of a health service provider, or

(b) a health service that affects the clinical management or care of a person who uses or receives a health service (including a patient).

(2) The Privacy Commissioner may communicate to the Health Care Complaints Commission any information that the Privacy Commissioner has obtained in relation to the complaint.

(3) The Privacy Commissioner and the Health Care Complaints Commission are to consult regularly to ensure the appropriate referral of complaints between them.

Note—

Section 26 of the *Health Care Complaints Act 1993* provides that the Health Care Complaints Commission may refer a complaint to another person or body. The Commission may therefore refer a complaint that raises a possible contravention of a Health Privacy Principle, a provision of Part 4 or a health privacy code of practice to the Privacy Commissioner.

(4) This section does not affect the operation of section 47 (Referring privacy related complaints to other authorities) of the PPIP Act.

66 Referring privacy related complaint to Commonwealth Privacy Commissioner

(1) The Privacy Commissioner may refer a complaint made under this Act to the Commonwealth Privacy Commissioner if it appears that the complaint should be dealt with by the Commonwealth Privacy Commissioner.

(2) The Privacy Commissioner may communicate to the Commonwealth Privacy Commissioner any information that the Privacy Commissioner has obtained in relation to the complaint.

(3) This section does not affect the operation of section 47 (Referring privacy related complaints to other authorities) of the PPIP Act.

67 Referring privacy related complaint to other persons or bodies

(1) The Privacy Commissioner may refer a complaint made under this Act for investigation or other action to any person or body (the ***relevant authority***) considered by the Privacy Commissioner to be relevant in the circumstances (other

than as provided by section 65 or 66).

(2) The Privacy Commissioner may communicate to the relevant authority any information that the Privacy Commissioner has obtained in relation to the complaint.

(3) The Privacy Commissioner may only refer a complaint to a relevant authority after appropriate consultation with the complainant and the relevant authority, and after taking their views into consideration.

(4) This section does not affect the operation of section 47 (Referring privacy related complaints to other authorities) of the PPIP Act.

Part 8 Miscellaneous

68 Corrupt disclosure or use of health information by public sector officials

(1) A public sector official must not, otherwise than in connection with the lawful exercise of his or her official functions, intentionally disclose or use any health information about an individual to which the official has or had access in the exercise of his or her official functions.

Maximum penalty—100 penalty units or imprisonment for 2 years or both.

(2) A person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any health information about an individual to which the official has or had access in the exercise of his or her official functions.

Maximum penalty—100 penalty units or imprisonment for 2 years or both.

(3) Subsection (1) does not prohibit a public sector official from disclosing any health information if the disclosure is made in accordance with the *Public Interest Disclosures Act 1994*.

(4) In this section, a reference to a public sector official includes a reference to a person who was formerly a public sector official.

Note—

Corrupt conduct by employees or agents of private sector persons in relation to health information may be dealt with under Part 4A (Corruptly receiving commissions and other corrupt practices) of the *Crimes Act 1900*.

69 Offering to supply health information that has been disclosed unlawfully

(1) A person who offers to supply (whether to a particular person or otherwise), or holds himself or herself out as being able to supply (whether to a particular person or otherwise), health information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 68 is guilty of an offence.

Maximum penalty—100 penalty units or imprisonment for 2 years, or both.

(2) If a person is convicted of an offence under section 68 or subsection (1), the court may order the confiscation of any money or other benefit alleged to have been obtained by the person in connection with the offence and for that money or other benefit to be forfeited to the Crown.

70 Intimidation, threats or misrepresentation

(1) A person must not, by threat, intimidation or misrepresentation, persuade or attempt to persuade an individual—

(a) to refrain from making or pursuing—

(i) a request for access to health information, or

(ii) a complaint to the Privacy Commissioner or the Tribunal under Part 6, or

(iii) an application under Part 5 of the PPIP Act with respect to the alleged contravention of a Health Privacy Principle or a health privacy code of practice, or

(b) to withdraw such a request, complaint or application.

Maximum penalty—100 penalty units.

(2) A person must not, by threat, intimidation or false representation, require another person—

(a) to give a consent under this Act, or

(b) to do, without consent, an act for which consent is required.

Maximum penalty—100 penalty units.

71 Legal rights not affected

(1) Nothing in this Act gives rise to, or can be taken into account in, any civil cause of action, and, without limiting the generality of the foregoing, nothing in this Act—

(a) operates to create in any person any legal rights enforceable in a court or tribunal otherwise than in accordance with the procedures set out in this Act, or

(b) affects the validity, or provides grounds for review, of any judicial or administrative act or omission.

(2) A contravention of this Act does not create any criminal liability except to the extent expressly provided by this Act.

72 Protection from liability

(1) Civil proceedings do not lie against a person in respect of loss, damage or injury of any kind suffered by another person by reason only of any of the following acts done in good faith—

(a) the making of a complaint or application under this Act,

(b) the making of a statement to, or the giving of a document or information to, the Privacy Commissioner, whether or not pursuant to a requirement under section 59 or 63.

(2) If an organisation provides an individual with access to health information under this Act, and the access was required by HPP 7 (Access to health information) or Part 4, or an employee, officer or agent of the organisation believed in good faith that the access was required by HPP 7 or a provision of Part 4—

(a) no action for defamation or breach of confidence lies against the organisation, any employee, officer or agent of the organisation or the Crown by reason of the provision of access, and

(b) no action for defamation or breach of confidence in respect of any publication involved in, or resulting from, the giving of access lies against the person who provided the health information to the organisation by reason of the person having supplied the health information to the organisation, and

(c) the organisation, or any employee, officer or agent of the organisation, or any other person concerned in giving access to the health information is not guilty of an offence merely because of the giving of access.

(3) The provision of access to health information in the circumstances referred to in subsection (2) must not be taken to constitute, for the purposes of the law relating to defamation or breach of confidence, an authorisation or approval of the publication of the health information by the person to whom access to the information is provided.

73 Fees

(1) An organisation may charge a fee for any of the following matters—

(a) giving an individual a copy of health information,

(b) giving an individual an opportunity to inspect and take notes of the health information,

(c) amending health information at the request of an individual,

(d) any other matter prescribed by the regulations.

(2) Any fee charged must not exceed such fee (if any) prescribed by the regulations for

the matter concerned.

74 Proceedings for offences

Proceedings for an offence against this Act are to be dealt with summarily before the Local Court.

75 Regulations

(1) The Governor may make regulations, not inconsistent with this Act, for or with respect to any matter that by this Act is required or permitted to be prescribed or that is necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Without limiting the generality of subsection (1), regulations may be made for or with respect to the following matters—

(a) disapplying any provision or provisions of Part 6 with respect to any private sector person or class of private sector persons, subject to subsection (3),

(b) the manner in which health privacy codes of practice are to be prepared and developed,

(c) exempting specified persons, private sector persons or public sector agencies, or classes of person, private sector persons or public sector agencies, from—

(i) any of the requirements of this Act or the regulations relating to the collection, use or disclosure of specified classes of health information, or

(ii) any other provision of this Act,

(d) providing for 2 or more public sector agencies or classes of public sector agencies to be treated as a single agency—

(i) for the purposes of this Act generally, or

(ii) for the purposes of specified provisions of this Act, or

(iii) for the purposes of specified Health Privacy Principles or health privacy codes of practice,

(e) providing for 2 or more private sector persons or classes of private sector persons (including private sector persons that are related bodies corporate) to be treated as a single private sector person—

(i) for the purposes of this Act generally, or

(ii) for the purposes of specified provisions of this Act, or

(iii) for the purposes of specified Health Privacy Principles or health privacy codes of practice,

(f) the auditing of compliance by organisations with the provisions of this Act, including the types of activities or conduct that may be subject to audit, the persons or bodies by whom an audit may be conducted and the frequency or timing of audits.

(3) A regulation made under subsection (2) (a) applies with respect to a private sector person only for so long as an individual is entitled to make a complaint that an act or practice by the private sector person may be an interference with the privacy of the individual (as referred to in section 13A of the *Privacy Act 1988* of the Commonwealth) under a Commonwealth privacy code binding the private sector person or class of private sector persons concerned that sets out procedures for making and dealing with complaints in relation to acts or practices of the private sector person or class of private sector persons.

(4) The regulations may create offences punishable by a penalty not exceeding 50 penalty units.

(5) In this section—

Commonwealth privacy code means a privacy code approved by the Commonwealth Privacy Commissioner under the *Privacy Act 1988* of the Commonwealth.

complaint means a complaint of any kind, regardless of the nature of any remedies that may be available in respect of the complaint.

75A Regulations with respect to healthcare identifiers

(1) Without limiting section 75, regulations may be made for or with respect to healthcare identifiers.

(2) In particular, the regulations may specify the circumstances in which a person may or may not use or disclose a healthcare identifier.

(3) A person who uses or discloses a healthcare identifier in contravention of a regulation made under subsection (2) is guilty of an offence.

Maximum penalty—

(a) 600 penalty units in the case of a body corporate, or

(b) 120 penalty units or imprisonment for 2 years, or both, in any other case.

76 Savings and transitional provisions

Schedule 2 has effect.

77 (Repealed)

78 Review of Act

(1) The Minister is to review this Act to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives.

(2) The review is to be undertaken as soon as possible after the period of 5 years from the date of assent to this Act.

(3) A report on the outcome of the review is to be tabled in each House of Parliament within 12 months after the end of the period of 5 years.

Schedule 1 Health Privacy Principles

(Section 4)

1 Purposes of collection of health information

(1) An organisation must not collect health information unless—

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

2 Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that—

(a) the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

3 Collection to be from individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4 Individual to be made aware of certain matters

(1) An organisation that collects health information about an individual from the

individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following—

(a) the identity of the organisation and how to contact it,

(b) the fact that the individual is able to request access to the information,

(c) the purposes for which the information is collected,

(d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind,

(e) any law that requires the particular information to be collected,

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that—

(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual, or

(b) the collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if—

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or

(b) the organisation is lawfully authorised or required not to comply with it, or

(c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or

(e) the information concerned is collected for law enforcement purposes, or

(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of

its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

5 Retention and security

(1) An organisation that holds health information must ensure that—

(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information.

Note—

Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if—

(a) the organisation is lawfully authorised or required not to comply with it, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) An investigative agency is not required to comply with subclause (1) (a).

6 Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain—

(a) whether the organisation holds health information, and

(b) whether the organisation holds health information relating to that individual, and

(c) if the organisation holds health information relating to that individual—

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

7 Access to health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Note—

Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Access to health information held by public sector agencies may also be available under the *Government Information (Public Access) Act 2009* or the *State Records Act 1998*.

(2) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

8 Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to

whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information—

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

Note—

Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Amendment of health information held by public sector agencies may also be able to be sought under the *Privacy and Personal Information Protection Act 1998*.

(4) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

9 Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

10 Limits on use of health information

(1) An organisation that holds health information must not use the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless—

(a) **Consent**

the individual to whom the information relates has consented to the use of the information for that secondary purpose, or

(b) **Direct relation**

the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or

Note—

For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(b1) **Emergency**

the use of the information for the secondary purpose meets the following conditions—

(i) the secondary purpose is to assist in a stage of an emergency,

(ii) the use of the information is reasonably necessary to assist in the stage of the emergency,

(iii) it is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates to the use of the information for the secondary purpose, or

(c) **Serious threat to health or welfare**

the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent—

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(c1) **Genetic information**

the information is genetic information and the use of the information for the secondary purpose—

(i) is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and

(ii) is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(d) **Management of health services**

the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and—

(i) either—

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**

the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and—

(i) either—

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**

the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and—

(i) either—

(A) that purpose cannot be served by the use of information that does not

identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Find missing person**

the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**

the organisation—

(i) has reasonable grounds to suspect that—

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(i) **Law enforcement**

the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(j) **Investigative agencies**

the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by

investigative agencies, or

(k) **Prescribed circumstances**

the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency—

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(4A) If health information is used under subclause (1)(b1), the organisation—

(a) must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained, and

(b) if the organisation is a law enforcement agency—must not use the information for the purpose of prosecuting an offence.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

11 Limits on disclosure of health information

(1) An organisation that holds health information must not disclose the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless—

(a) **Consent**

the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

(b) **Direct relation**

the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

Note—

For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(b1) **Emergency**

the disclosure of the information for the secondary purpose meets the following conditions—

(i) the secondary purpose is to assist in a stage of an emergency,

(ii) the disclosure of the information is reasonably necessary to assist in the stage of the emergency,

(iii) it is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates to the disclosure of the information for the secondary purpose, or

(c) **Serious threat to health or welfare**

the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent—

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(c1) **Genetic information**

the information is genetic information and the disclosure of the information for the secondary purpose—

(i) is to a genetic relative of the individual to whom the genetic information relates, and

(ii) is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat

is imminent) of a genetic relative of the individual to whom the genetic information relates, and

(iii) is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(d) **Management of health services**

the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and—

(i) either—

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**

the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and—

(i) either—

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**

the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and—

(i) either—

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) the information will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Compassionate reasons**

the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and—

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) the individual is incapable of giving consent to the disclosure of the information, and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Find missing person**

the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**

the organisation—

(i) has reasonable grounds to suspect that—

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**

the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(k) **Investigative agencies**

the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) **Prescribed circumstances**

the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their

investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency—

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(5A) If health information is disclosed under subclause (1)(b1), the organisation—

(a) must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained, and

(b) if the organisation is a law enforcement agency—must not use the information for the purpose of prosecuting an offence.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

12 Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if—

(a) the individual has consented to the adoption of the same identifier, or

(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if—

(a) the use or disclosure is required for the purpose for which it was assigned or for a

secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)–(k) or 11 (1) (c)–(l), or

(b) the individual has consented to the use or disclosure, or

(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either—

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or

(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

14 Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless—

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or

(b) the individual consents to the transfer, or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

(e) all of the following apply—

(i) the transfer is for the benefit of the individual,

(ii) it is impracticable to obtain the consent of the individual to that transfer,

(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent—

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

15 Linkage of health records

(1) An organisation must not—

(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if—

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause—

health record means an ongoing record of health care for an individual.

health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

16 (Repealed)

Schedule 2 Savings and transitional provisions

(Section 76)

1 Regulations

(1) The regulations may contain provisions of a savings or transitional nature consequent on the enactment of the following Acts—

this Act

Health Legislation Further Amendment Act 2010

(2) Without limiting subclause (1), the regulations may make provision for or with respect to the following matters—

(a) exempting organisations or classes of organisations from the operation of this Act in connection with the performance of contracts entered into before the date of assent to this Act,

(b) providing that a privacy code of practice dealing with health information in force under the *Privacy and Personal Information Protection Act 1998* is taken to be a health privacy code of practice in force under this Act.

(3) Any provision referred to in subclause (1) may, if the regulations so provide, take effect from the date of assent to the Act concerned or a later date.

(4) To the extent to which any such provision takes effect from a date that is earlier than the date of its publication in the Gazette, the provision does not operate so as—

(a) to affect, in a manner prejudicial to any person (other than the State or an authority of the State), the rights of that person existing before the date of its publication, or

(b) to impose liabilities on any person (other than the State or an authority of the State) in respect of anything done or omitted to be done before the date of its publication.

2 Privacy Commissioner may exempt

The Privacy Commissioner may, on application by an organisation, grant the organisation an exemption from the operation of HPP 10 or 11 in relation to specified information (or information of a specified class for a specified period) collected by the organisation before the commencement of this clause if—

(a) the Privacy Commissioner is of the opinion that, in the particular circumstances, it is in the public interest for the use or disclosure to continue otherwise than in accordance with HPP 10 or 11, and

(b) the period of any exemption expires before the second anniversary of the commencement of this clause.

Schedule 3 (Repealed)