



HEALTH DATA PROTECTION REGULATION

REGULATION NUMBER (7) OF 2008

Table of Contents.....Error! Bookmark not defined.

Part One : Preliminary and Key Provisions 5

1 Title..... 5

2 Issue of Regulation 5

3 Amendment to Regulations 5

4 Hierarchy 5

5 Commencement..... 5

6 Background 5

7 Purpose 5

8 Application of this Health Data Protection Regulation 6

9 Requirement to comply with Regulations 6

10 Health Data Protection Regulation to be read in conjunction with other Regulations 6

11 Responsibility for administration of Regulations 7

Part Two : Interpretation 8

12 Definitions..... 8

13 Regulations include amendments..... 9

14 Headings..... 10

15 Gender..... 10

16 Documents in languages other than English 10

17 Documents in writing..... 10

18 Meaning of person..... 10

19 Reference to sections and subsections 10

Part Three : General Provisions..... 11

20 Patient Health Information held by Licensees..... 11

21 Patient Health Information held by employee, contractor or member..... 11

22 Patient Health Information held by agent or for safe custody or processing 11

23 Disclosure of Patient Health Information to staff of a Licensee 11

Part Four : Health Data Protection Principles 12

24 Health Data Protection Principles 12

Principle 1 Purpose of Collection of Patient Health Information 12

Principle 2 Source of Health Information..... 12

Principle 3 Collection of Patient Health Information from Patient..... 13

Principle 4 Manner of Collection of Patient Health Information 14

Principle 5 Storage and Security of Patient Health Information 14

Principle 6 Access to Patient Health Information	15
Principle 7 Correction of Patient Health Information	15
Principle 8 Accuracy of Patient Health Information to be checked before use	16
Principle 9 Retention of Patient Health Information	16
Principle 10 Limits on Use of Patient Health Information	16
Principle 11 Limits on Disclosure of Patient Health Information.....	17
Principle 12 Personal Identifiers.....	20
25 Data Protection Officers	20
26 Savings	20
Part Five : Health Data Protection Ombudsman	21
27 Health Data Protection Ombudsman.....	21
28 Appointment of the Health Data Protection Ombudsman	21
29 Removal of the Health Data Protection Ombudsman	21
30 Resignation of the Health Data Protection Ombudsman	21
31 Powers and Functions of the Health Data Protection Ombudsman	21
32 Production of Information	23
33 Rules, Standards and Policies.....	23
34 Funding and fees.....	23
35 Annual Funding of the Health Data Protection Ombudsman.....	23
36 Accounts.....	24
37 Annual Report	24
Part Six : Procedural provisions relating making a request to access and correction Patient Health Information.....	25
38 Patient Data Requests	25
39 Who may make requests?.....	25
40 Form of request.....	25
41 No charge for Patient Data Requests	25
42 Charges may be made for certain Patient Health Information.....	25
43 Urgency	26
44 Assistance.....	26
45 Transfer of requests	26
46 Decisions on requests.....	26
47 Extension of time limits	26
48 Form for making information available	27
49 Deletion of information from Documents.....	27
50 Reason for refusal to be given.....	28
51 Precautions before releasing Patient Health Information	28

Part Seven : Good reasons for refusing access to Patient Health Information..	29
52 Grounds for refusing access to Patient Health Information	29
Part Eight : Electronic Health Record.....	31
53 Establishment of an Electronic Health Record	31
54 Certain information from Electronic Health Record to be used for HIRAS	31
55 HIRAS compliance with this Regulation	31
56 Purpose of HIRAS	31
57 Requirement to provide information	31
58 Source of the Patient Health Information.....	31
59 Patient awareness.....	32
Part Nine : Transfer of Patient Health Information	33
60 Transfer of Patient Health Information out of DHCC.....	33
61 Meaning of adequate level of protection.....	33
Part Ten : Interference with a Patient’s Patient Health Information	34
62 Interference with Patient Health Information.....	34
Part Eleven : Complaints	35
63 Complaints relating to an Interference with Patient Health Information	35
64 Complaints	35
65 Referral of complaint to the Executive Committee.....	35
66 Referral of Complaint by Executive Committee.....	35
67 Complainant may refer the complaint to the Health Data Protection Ombudsman 35	
68 Action on receipt of complaint	35
69 Health Data Protection Ombudsman may decide to take no action on complaint	35
70 Proceedings of Health Data Protection Ombudsman.....	36
71 Settlement of complaints	36
72 Parties to be informed of result of investigation.....	36
73 Procedure after investigation.....	37
74 Health Data Protection Ombudsman to report Licensee not meeting the Regulation requirements.....	37
75 Compliance with requirements of Health Data Protection Ombudsman	37

Part One : Preliminary and Key Provisions

1 Title

This regulation is to be referred to as the DHCC Health Data Protection Regulation No. (7) of 2008 (the Health Data Protection Regulation).

2 Issue of Regulation

This Health Data Protection Regulation is issued in accordance with Article 9 of Decree no.(9) of 2003 and adopted under Order no (1) of 2008.

3 Amendment to Regulations

The Chairman may, from time to time, amend this Health Data Protection Regulation in accordance with the provisions of the Governing Regulation.

4 Hierarchy

- (1) If there is any conflict between the provisions of this Health Data Protection Regulation and the Governing Regulation adopted by the Chairman, the provisions of this Regulation will prevail.
- (2) In the event of any inconsistency between an earlier version of a Regulation and an amended version of the same Regulation, the most recently amended version of the Regulation will prevail.

5 Commencement

This Health Data Protection Regulation comes into force on the date of its issuance by the Chairman.

6 Background

- (1) Health information is a core component of a functioning health system and evidence-based decision-making.
- (2) Health information is produced from various data sources, which may be the responsibility of different Entities and Licensees. It must be managed in an integrated way to maximize effectiveness and efficiency in the delivery of Healthcare Services.
- (3) Internationally, different countries have implemented protections around the management of Patient Health Information, recognizing that the flow of Patient Health Information is vital to the delivery of an integrated health service.
- (4) This Regulation is based on the protection of personal information and Patient Health Information found in the:
 - (a) Organisation for Economic Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;
 - (b) European Parliament Directives regarding the protection of personal data;
 - (c) Asia-Pacific Economic Cooperation (APEC) Privacy Framework; and
 - (d) Health Insurance Portability and Accountability (HIPPA) Privacy Rule.

7 Purpose

- (1) The purpose of this Regulation is to promote and protect Patient Health Information and in particular to:

-
- (a) establish certain principles with respect to the collection, use and disclosure by the DHCCA and Licensees within DHCC, of Patient Health Information;
 - (b) establish certain principles with respect to access by each Patient to his Patient Health Information held by DHCCA and Licensees;
 - (c) create a safe environment where health information systems are used to produce relevant and good quality information in support of the delivery of Healthcare Services;
 - (d) promote a flexible approach to the protection of Patient Health Information while avoiding the creation of unnecessary barriers to the flow of Patient Health Information to appropriate parties;
 - (e) establish a complaints mechanism for the investigation of complaints regarding Patient Health Information.

8 Application of this Health Data Protection Regulation

- (1) This Health Data Protection Regulation applies to all Licensees in their management of Patient Health Information regardless of where that information might be held.
- (2) It is a requirement that Licensees must comply with the Health Data Protection Regulation and Rules and Policies made under the Health Data Protection Regulation with regard to Patient Health Information.
- (3) This Data Protection Regulation applies to the following types of Patient Health Information:
 - (a) information about the health of a patient, including his medical history;
 - (b) information about any disabilities that patient has, or has had;
 - (c) information about any Healthcare Services that are being provided, or have been provided, to that patient;
 - (d) information provided by that patient in connection with the donation, by that patient, of any body part or any bodily substance of that patient, or derived from the testing or examination of any body part, or any bodily substance of that patient; or
 - (e) information about that patient which is collected before, or in the course of, and incidental to, the provision of any Healthcare Service to that patient.

9 Requirement to comply with Regulations

It is a requirement that any Applicant, Provisional Clinical Operating Permit Holder, or Licensee must comply with, submit to and be bound by the relevant Regulations, the applicable Rules or Standards, and all applicable Policies.

10 Health Data Protection Regulation to be read in conjunction with other Regulations

- (1) This Health Data Protection Regulation should be read in conjunction with the following Regulations and any amendments to such Regulations:
 - (a) Commercial Services Licensing Regulation;
 - (b) Company Regulations;
 - (c) Complementary and Alternative Medicine Regulation; and
 - (d) Education Regulation;

-
- (e) Governing Regulation;
 - (f) Healthcare Operator Regulation;
 - (g) Healthcare Professionals Regulation;
 - (h) Medical Liability Regulation;
 - (i) Research Regulation;
 - (j) Any other Regulations adopted by the Chairman under the Decree.

11 Responsibility for administration of Regulations

- (1) This Health Data Protection Regulation is administered by the Health Data Protection Ombudsman and pending the appointment of such an Ombudsman the Board of Directors and the Executive Committee through CPQ are responsible for administering this Regulation.
- (2) During the period prior to the appointment of the Health Data Protection Ombudsman, all references within the Regulation to the Health Data Protection Ombudsman will refer to the chairman of the Board of Directors who may delegate such responsibilities.

Part Two : Interpretation

12 Definitions

Capitalized terms not defined in this Health Data Protection Regulation shall have the meanings ascribed to them in the Governing Regulation. Unless it is specifically stated otherwise in another Regulation or unless the context otherwise requires:

Action includes failure to act;

Collect, Collection, Collected means the obtaining of Patient Health Information directly from the Patient or in accordance with section 24, Principle 2 of this Regulation and for the avoidance of doubt does not include receipt of unsolicited information;

Correct, in relation to Patient Health Information, means to alter that information by way of correction, deletion, or addition; and correction has a corresponding meaning;

Data Protection Principle means any of the Data Protection Principles set out in section 24;

Data Protection Officer means the person appointed under section 25 to carry out the functions set out in section 25;

Data Stewards means the people who are identified by position in the relevant Policies as being responsible for ensuring that security of Patient Health Information held by DHCCA and CPQ;

Document has the meaning as defined in the Governing Regulations and for the purpose of this Regulation includes the reports from photographs, x-ray films, scans, recordings and other such diagnostic procedures;

Electronic Health Record means longitudinal, patient-centered, shared care records, to which all relevant parties contribute and have access electronically, for the purposes of enabling continuity of care throughout a network of Licensed Healthcare Professionals, Licensed Complementary and Alternative Medicine Providers and Licensed Healthcare Operators;

Health Data Protection Ombudsman means the person appointed under section 27 to carry out the functions set out in section 27;

HIRAS or Healthcare Information Reporting and Analysis System means the health information system, which is a sub set of the Electronic Health Record, maintained and used by CPQ to collect patient information from Licensees for quality, licensing, medical educational, research and other purposes;

Hospital Information System means an information system that encompasses the clinical and non-clinical activities used by Licensed Healthcare Operators;

Interference with Patient Health Information has the meaning given to it in section 62;

Minimum Dataset Requirement Policy means the Policy setting out the Minimum Required Data Submission Requirements;

Minimum Required Data Submission Requirements means the requirements approved by the Clinical Governance Board relating to minimum datasets required to be submitted for inclusion on HIRAS;

Patient means with respect to Patient Health Information, the Patient to whom such Patient Health Information relates;

Patient Data Request has the meaning given to it under section 38 of these Regulations;

Patient Health Information has the meaning given to it under the Governing Regulation;

Personal identifier means an identifier that:

- i. is assigned to a patient by a Licensee for the purposes of the operations of the Licensee and the Agencies; and
- ii. uniquely identifies that Patient in relation to the Licensee and Agencies;

however, for the avoidance of doubt, does not include a patient's name used to identify that Patient;

Process, Processed, Processes and Processing means any operation or set of operations which is performed on Patient Health Information, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, erasure or destruction;

Publicly Available Information means Patient Health Information that is contained in a Publicly Available Publication;

Publicly Available Publication means a magazine, book, newspaper, report or other Document that is or will be generally available to member of the public;

Representative, in relation to a Patient, means:

- i. where that Patient is dead, that Patient's executor or administrator;
- ii. where the Patient is under the age of sixteen (16) years – that Patient's parent or guardian; or
- iii. where the Patient, not being a Patient referred to in (i) or (ii), is unable to give his authorization, or exercise his rights, a person appearing to be lawfully acting on the Patient's behalf or in his interests;

Research Ethics Review Committee is a committee set up under the Research Regulations.

13 Regulations include amendments

References in this Health Data Protection Regulation are to be read as including any amendments to this Regulation.

14 Headings

The headings used in this Health Data Protection Regulation are included for convenience of reference only and shall be ignored in the construction or interpretation of this Regulation.

15 Gender

Pronouns indicating male gender are used to refer to persons of both genders.

16 Documents in languages other than English

A person who wishes to submit an original document, a photocopy or an electronic version of a document written in a language other than English must also submit a notarized translation into English of such document prepared by a translation service acceptable to the officer, employee or agent providing the DHCCA Services to whom the document is submitted.

17 Documents in writing

References in Regulations to any requirement for any document to be written, in writing, to be presented in writing or for the giving of any notice are to be construed as being satisfied by an Electronic Record and any references in Regulations to any requirement for a signature on any document or notice are to be construed as being satisfied by an Electronic Signature that may be proved in a manner satisfactory to the officer, employee or agent providing the DHCCA Services who is the recipient of such document.

18 Meaning of person

Unless the context otherwise requires, any reference in Regulations to a “person” includes a reference to a natural person, and to a body corporate, limited liability company, association or partnership and to the legal or personal representatives, legal successors and lawful assigns of any such person.

19 Reference to sections and subsections

Unless otherwise specifically stated, references in this Regulation to a section and subsection mean the section and subsection of this Regulation.

Part Three : General Provisions

20 Patient Health Information held by Licensees

For the purposes of this Health Data Protection Regulation, a Licensee holds Patient Health Information if the information is contained in a Document that is in the possession or under the control of the Licensee whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside DHCC.

21 Patient Health Information held by employee, contractor or member

Patient Health Information that is held by an employee, contractor or member of a Licensee in that person's capacity as such an employee, contractor or member, will be deemed for the purposes of this Health Data Protection Regulation to be held by the Licensee of which that person is an officer, employee, contractor or member.

22 Patient Health Information held by agent or for safe custody or processing

(1) For the purposes of this Regulation, the Patient Health Information will be deemed to be held by the Licensee on whose behalf that Patient Health Information is so held or, as the case may be, is so Processed where a Licensee holds Patient Health Information:

- (a) solely as the agent of another Licensee; or
- (b) for the sole purpose of safe custody; or
- (c) for the sole purpose of Processing the Patient Health Information on behalf of another Licensee; and
- (d) does not use or disclose the Patient Health Information for its own purposes.

23 Disclosure of Patient Health Information to staff of a Licensee

For the purposes of this Regulation, an Action done by, or Patient Health Information disclosed to, a person employed by, or in the services of, a Licensee in the performance of the duties of the person's employment shall be treated as having been done by, or disclosed to, the Licensee.

Part Four : Health Data Protection Principles

24 Health Data Protection Principles

Principle 1

Purpose of Collection of Patient Health Information

- (1) Patient Health Information must not be collected by any Licensee unless the:
 - (a) Patient Health Information is collected for a lawful purpose connected with a function or activity of the Licensee; and
 - (b) collection of the Patient Health Information is necessary for that purpose.
- (2) Where a Licensee is to attach a Personal Identifier to the Patient Health Information to enable the linking of Patient Health Information from different Health Agencies, the Licensee must define the purpose of such linking of Patient Health Information.

Principle 2

Source of Health Information

- (1) Where a Licensee collects Patient Health Information, the Licensee must collect the Patient Health Information directly from the Patient concerned.
- (2) It is not necessary for a Licensee to comply with sub principle (1) if the Licensee believes on reasonable grounds that:
 - (a) the Patient concerned authorizes collection of the information from someone else having been made aware of the matters set out in sub principle 3(1);
 - (b) the Patient is unable to give his authority, and the Licensee having made the Patient's Representative aware of the matters set out in sub principle 3(1) collects the Patient Health Information from the Representative or the Representative authorizes collection from someone else;
 - (c) compliance would prejudice the:
 - (i) interests of the Patient; or
 - (ii) purposes of collection; or
 - (iii) safety of any individual;
 - (d) compliance is not reasonably practicable in the circumstances of the particular case;
 - (e) the collection is for the purpose of assembling a family or genetic history of a Patient and is collected directly from that Patient;
 - (f) the Patient Health Information is Publicly Available Information;
 - (g) the Patient Health Information:
 - (i) will not be used in a form in which the Patient is identified;
 - (ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the Patient; or
 - (iii) will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the Patient;

-
- (h) non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law including the prevention, detection, investigation, prosecution, and punishment of offences;
 - (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation).

Principle 3
Collection of Patient Health Information from Patient

- (1) Where an Licensee collects Patient Health Information directly from the Patient, or from the Patient's Representative, the Licensee must take such steps as are, in the circumstances, reasonable, to ensure that the Patient (and the Representative if collection is from the Representative) is aware of the:
 - (a) fact that the Patient Health Information is being collected;
 - (b) purpose for which the Patient Health Information is being collected;
 - (c) intended recipients of the Patient Health Information, including the provision of Patient Health Information for inclusion in any Electronic Health Record;
 - (d) name and address of the Licensee that:
 - (i) is collecting the Patient Health Information; and
 - (ii) will hold the Patient Health Information;
 - (e) whether or not the supply of the Patient Health Information is voluntary or mandatory;
 - (f) the consequences (if any) for that Patient if all or any part of the requested Patient Health Information is not provided; and
 - (g) the rights of access to, and correction of, Patient Health Information provided by principles 6 and 7.
- (2) The steps referred to in sub principle (1) must be taken before the Patient Health Information is collected, or, if that is not practicable, as soon as practicable after it is collected.
- (3) A Licensee is not required to take the steps referred to in sub principle (1) in relation to the collection of Patient Health Information from a Patient, or the Patient's representative, if that Licensee has taken those steps in relation to the collection, from that Patient or that Representative, of the same Patient Health Information or Patient Health Information of the same kind for the same or a related purpose, on a recent previous occasion.
- (4) It is not necessary for a Licensee to comply with sub principle (1) if the Licensee believes on reasonable grounds that:
 - (a) compliance would prejudice the:
 - (i) interests of the Patient; or
 - (ii) purposes of collection;
 - (b) compliance is not reasonably practicable in the circumstances of the particular case; or
 - (c) non-compliance is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution, and punishment of offences.

Principle 4
Manner of Collection of Patient Health Information

- (1) Patient Health Information must not be collected by a Licensee by:
 - (a) unlawful means; or
 - (b) means that, in the circumstances of the case:
 - (i) are unfair; or
 - (ii) intrude to an unreasonable extent upon the personal affairs of the Patient.

Principle 5
Storage and Security of Patient Health Information

- (1) A Licensee is responsible for the security of its information systems and networks and should:
 - (a) act in a timely and co-operative manner to prevent detect and respond to security incidents;
 - (b) review and assess the security of information systems and networks and make appropriate modifications to security policies, practices, measures and procedures on a regular basis;
 - (c) Periodically disclose security incidents to the Health Data Protection Ombudsman on the request of the Health Data Protection Ombudsman.
- (2) A Licensee must incorporate security as an essential element of information systems and networks.
- (3) A Licensee that holds Patient Health Information must ensure that:
 - (a) Patient Health Information is stored in a manner that enables the sharing of relevant information for the provision of Healthcare Services to a Patient by Licensed Healthcare Professionals and Licensed Complementary and Alternative Medicine Providers;
 - (b) Patient Health Information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:
 - (i) loss;
 - (ii) unauthorized access, use, modification, or disclosure; and
 - (iii) other misuse;
 - (c) if it is necessary for the Patient Health Information to be given to a person in connection with the provision of a service to the Licensee, including any storing, Processing, or destruction of the Patient Health Information, everything reasonably within the power of the Licensee is done to prevent unauthorized use or unauthorized disclosure of the Patient Health Information; and
 - (d) where a Document containing Patient Health Information is not to be kept or is no longer required to be retained, the Document is disposed of in a secure manner that preserves the privacy of the Patient.
- (4) When disclosing Patient Health Information in accordance with this Regulation over a telephone, the Licensed Healthcare Professional or Licensed Healthcare Practitioner must take safeguards to ensure that the information is not disclosed to any person other than the intended recipient.

-
- (5) Patient Health Information may only be disclosed by facsimile in accordance with this Regulation once the Licensed Healthcare Professional or Licensed Healthcare Practitioner has verified the identity of the intended recipient and confirmed the facsimile number as correct.
 - (6) Patient Health Information may only be disclosed electronically in accordance with DHCCA Rules, Policies and Standards.
 - (7) This principle applies to Patient Health Information obtained before or after the commencement of this Health Data Protection Regulation.

Principle 6
Access to Patient Health Information

- (1) Where a Licensee holds Patient Health Information in such a way that it can readily be retrieved, the Patient is entitled to:
 - (a) obtain from the Licensee confirmation of whether or not the Licensee holds such Patient Health Information; and
 - (b) have access to that Patient Health Information.
- (2) Where, in accordance with sub principle (1)(b), a Patient is given access to his Patient Health Information, the Patient must be advised that, under principle 7, the Patient may request the correction of that information.
- (3) The application of this principle is subject to:
 - (a) Part 6 of this Regulation which sets out procedural provisions relating to access to information;
 - (b) sections 41 and 42 which concern charges;
 - (c) section 52 which sets out reasons for withholding information.
- (4) This principle applies to Patient Health Information obtained before or after the commencement of this Health Data Protection Regulation.

Principle 7
Correction of Patient Health Information

- (1) Where a Licensee holds Patient Health Information, the Patient concerned is entitled to request:
 - (a) correction of the Patient Health Information; and
 - (b) that there be attached to the Patient Health Information a statement of the correction sought but not made.
- (2) A Licensee that holds Patient Health Information must, if so requested or on its own initiative, take such steps (if any) to correct the Patient Health Information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the Patient Health Information may lawfully be used, it is accurate, up to date, complete, and not misleading.
- (3) Where a Licensee that holds Patient Health Information is not willing to correct the Patient Health Information in accordance with such a request, the Licensee must, if so requested, take such steps (if any) as are reasonable to attach to the Patient Health Information, in such a manner that it will always be read with the information, any statement provided by the Patient of the correction sought.
- (4) Where the Licensee has taken steps under sub principle (2) or (3), the Licensee must, if reasonably practicable, inform each person or body or

Licensee to whom the Patient Health Information has been disclosed of those steps.

- (5) Where a Licensee receives a request made under sub principle (1), the Licensee must inform the Patient concerned of the Action taken as a result of the request.
- (6) The application of this principle is subject to the provisions of Part 6.
- (7) This principle applies to Patient Health Information obtained before or after the commencement of this Health Data Protection Regulation.

Principle 8

Accuracy of Patient Health Information to be checked before use

- (1) A Licensee that holds Patient Health Information must not use that Patient Health Information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the Patient Health Information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.
- (2) This principle applies to Patient Health Information obtained before or after the commencement of this Health Data Protection Regulation.

Principle 9

Retention of Patient Health Information

- (1) A Licensee must retain Patient Health Information in a secure environment for a minimum of ten (10) years beginning on the day after the date shown in the Patient Health Information as the most recent date on which a Licensee provided Healthcare Services to the Patient.
- (2) Sub principle (1) does not apply to the actual photographs, films, scans, recordings and other such diagnostic procedures of a similar type that are obtained for diagnostic purposes; however sub-principle (1) does apply to the report obtained as the result of such diagnostic procedures.
- (3) Subject to sub principle (1) a Licensee that holds Patient Health Information must not keep that Patient Health Information for longer than is required for the purposes for which the Patient Health Information may lawfully be used.
- (4) Sub principle (1) does not prohibit any Licensee from keeping any document that contains Patient Health Information, where the retention of such a document is necessary or desirable for the purposes of providing Healthcare Services to the Patient.
- (5) This principle applies to Patient Health Information obtained before or after the commencement of this Health Data Protection Regulation.

Principle 10

Limits on Use of Patient Health Information

- (1) A Licensee that holds Patient Health Information obtained in connection with one purpose must not use the Patient Health Information for any other purpose unless the Licensee believes on reasonable grounds that the:
 - (a) use of the Patient Health Information for that other purpose is authorized by the:
 - (i) Patient; or

-
- (ii) Patient's Representative where the Patient is unable to give his authority under this principle;
 - (b) purpose for which the Patient Health Information is used is directly related to the purpose in connection with which the Patient Health Information was obtained;
 - (c) source of the Patient Health Information is a Publicly Available Publication;
 - (d) use of the Patient Health Information for that other purpose is necessary to prevent or lessen a serious and imminent threat to:
 - (i) public health or public safety; or
 - (ii) the life or health of the Patient concerned or another individual;
 - (e) Patient Health Information is used:
 - (i) in a form in which the Patient is not identified;
 - (ii) for statistical purposes and will not be published in a form that could reasonably be expected to identify the Patient; or
 - (iii) for research purposes (for which approval by the Research Ethics Review Committee or another ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the Patient;
 - (f) non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution, and punishment of offences; or
 - (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
- (2) This principle does not apply to Patient Health Information obtained before this Health Data Protection Regulation comes into force.

Principle 11
Limits on Disclosure of Patient Health Information

- (1) An Licensee that holds Patient Health Information must not disclose the Patient Health Information unless the Licensee believes, on reasonable grounds that the:
- (a) disclosure is to the Patient, or the Patient's Representative where the Patient is dead or is unable to exercise his rights under these principles;
 - (b) disclosure is authorized by the Patient, or the Patient's Representative where the Patient is dead or is unable to give his authority under this principle;
 - (c) disclosure is one of the purposes in connection with which the information was obtained;
 - (d) disclosure is to a Licensed Healthcare Professional or Licensed Complementary and Alternative Medicine Provider that is providing or is to provide, Healthcare Services to the Patient and includes disclosing Patient Health Information for the following purposes:
 - (i) provision of treatment in emergency situations;

-
- (ii) Patient transfers;
 - (iii) discharge planning;
 - (iv) ensuring the coordination of Healthcare Services to the Patient;
 - (e) source of the Patient Health Information is a Publicly Available Publication;
 - (f) Patient Health Information is in general terms, concerning the presence, location, and condition and progress of the Patient in a Healthcare facility within DHCC, on the day on which the Patient Health Information is disclosed, and the disclosure is not contrary to the express request of the Patient or his Representative;
 - (g) the Patient Health Information to be disclosed concerns only the fact of death and the disclosure is by a Licensed Healthcare Professional, or by a person authorized by a Licensee, to a person nominated by the Patient, or the Patient's Representative, spouse, principal caregiver, next of kin, close relative or other person whom it is reasonable in the circumstances to inform; or
 - (h) Patient has a communicable disease which falls into the category of diseases which require notification to the Dubai Health Authority.
- (2) Compliance with sub principle (1)(b) is not necessary if the Licensee believes on reasonable grounds that it is either not desirable or not practicable to obtain authorization from the Patient and that the:
- (a) disclosure of the Patient Health Information is directly related to one of the purposes in connection with which the Patient Health Information was obtained;
 - (b) Patient Health Information is disclosed by a Licensed Healthcare Professional to a person nominated by the Patient or to the principal caregiver or a near relative of the Patient concerned in accordance with recognized professional practice and the disclosure is not contrary to the express request of the Patient or his Representative;
 - (c) information is to be used:
 - (i) in a form in which the Patient is not identified;
 - (ii) for statistical purposes and will not be published in a form that could reasonably be expected to identify the Patient; or
 - (iii) for research purposes (for which approval by the Research Ethics Review Committee or another ethics committee, if required, has been given), and will not be published in a form which could reasonably be expected to identify the Patient;
 - (d) disclosure of the Patient Health Information is necessary to prevent or lessen a serious and imminent threat to:
 - (i) public health or public safety; or
 - (ii) the life or health of the Patient or another individual;
 - (e) disclosure of the Patient Health Information is essential to facilitate the sale or other disposition of a business as a going concern;

-
- (f) Patient Health Information to be disclosed briefly describes only the nature of injuries of an Patient sustained in an accident and that Patient's identity and the disclosure is:
 - (i) by a person authorized by the person in charge of a hospital;
 - (ii) to a person authorized by the person in charge of a news medium; for the purpose of publication or broadcast in connection with the news activities of that news medium and the disclosure is not contrary to the express request of the Patient or his representative;
 - (g) disclosure of the Patient Health Information is:
 - (i) required for the purposes of identifying whether a Patient is suitable to be involved in health education and so that Patients so identified may be able to be contacted to seek their authority in accordance with paragraph (1)(b); and
 - (ii) by a person authorized by the Licensee to an Approved Education Operator;
 - (h) disclosure of the Patient Health Information is required for:
 - (i) the purpose of a professionally recognized accreditation of a Healthcare Service;
 - (ii) a professionally recognized external quality assurance programme; or
 - (iii) risk management assessment and the disclosure is solely to a person engaged by the Licensee for the purpose of assessing the Licensee's risk

and the Patient Health Information will not be published in a form which could reasonably be expected to identify any Patient, nor disclosed by the accreditation or quality assurance or risk management organization to third parties except as required by law;
 - (i) non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law including the prevention, detection, investigation, prosecution and punishment of offences; or
 - (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
 - (j) Patient is or is likely to become dependent upon a controlled drug, prescription medicine or restricted medicine and the disclosure is by a Licensed Healthcare Professional to DHCCA for the purposes of taking the appropriate action.
- (3) Disclosure under sub principle (2) is permitted only to the extent necessary for the particular purpose.
 - (4) Where there is disclosure of Patient Health Information under sub principle (2), the Licensee will as soon as practicable:
 - (a) notify the Patient of the disclosure of Patient Health Information;
 - (b) if the disclosure relates to a claim by a Patient about a Licensee, notify CPQ of the disclosure of the Patient Health Information.

-
- (5) This principle applies to Patient Health Information about living or deceased persons, obtained before or after the commencement of this Health Data Protection Regulation.
 - (6) Despite sub principle (5), a Licensee is exempted from compliance with this principle in respect of Patient Health Information about an identifiable deceased person who has been dead for more than twenty (20) years.
 - (7) For the avoidance of doubt, disclosure of Patient Health Information may be either verbal or written.

**Principle 12
Personal Identifiers**

- (1) A Licensee may assign a Personal Identifier to Patient when the assignment of that identifier is necessary to enable the Licensee to carry out any one or more of its functions efficiently.
- (2) The Licensing Board and CPQ may assign a Personal Identifier to a Licensed Healthcare Professional or a Licensed Complementary and Alternative Medicine Provider to enable the Licensing Board and CPQ to carry out any one or more of its functions efficiently.
- (3) When assigning a Personal Identifier, a Licensee, or the Licensing Board, or CPQ, must take all reasonable steps to ensure that the Personal Identifier is assigned only to Patients, Licensed Healthcare Professionals and Licensed Complementary and Alternative Medicine Providers whose identity has been clearly established.
- (4) In accordance with sub principle 1 and sub principle 3, a Licensee, the Licensing Board, or CPQ, must ensure that the Patient, Licensed Healthcare Professional and a Licensed Complementary and Alternative Medicine Provider is made aware of the purposes of the assignment of the Personal Identifier and the intended subsequent use of the Personal Identifier.
- (5) The collection, storage, use and disclosure of a Personal Identifier assigned to a Patient and the Patient Health Information, attached to the Personal Identifier must be in accordance with the provisions of this Health Data Protection Regulation.

25 Data Protection Officers

- (1) It shall be the responsibility of each Licensee to ensure that there are, within that Licensee, one or more individuals whose responsibilities include:
 - (a) the encouragement of compliance, by the Licensee, with the Health Data Protection Principles;
 - (b) dealing with requests made to the Licensee under this Health Data Protection Regulation;
 - (c) otherwise ensuring compliance by the Licensee with the provisions of this Health Data Protection Regulation.

26 Savings

An action is not a breach of any of the principles if that action is authorized or required by or under another Regulation.

Part Five : Health Data Protection Ombudsman

27 Health Data Protection Ombudsman

- (1) The Chairman will appoint a person who is appropriately experienced and qualified to be the Health Data Protection Ombudsman.
- (2) The Health Data Protection Ombudsman is responsible for the administration of this Regulation and may appoint any appropriate person to discharge his duties and exercise his powers under this Regulation.
- (3) The Health Data Protection Ombudsman will develop and carry out policies to promote greater awareness of this Regulation.
- (4) The Health Data Protection Ombudsman, by conditional or unconditional written authority, may delegate the Health Data Protection Ombudsman's powers and duties under this Regulation to any appropriate person employed under section 27(2).
- (5) A person to whom the Health Data Protection Ombudsman, delegates powers and duties, by written authority under section 27(4), may exercise the powers and shall perform the duties in accordance with the written authority.

28 Appointment of the Health Data Protection Ombudsman

- (1) The Chairman will consult with the Board of Directors prior to appointing, re-appointing or dismissing the Health Data Protection Ombudsman.
- (2) The Health Data Protection Ombudsman will be appointed for a specified period of time not exceeding three (3) years, and may be re-appointed provided that such period may not extend beyond the day when the Health Data Protection Ombudsman turns seventy-five (75) years of age.
- (3) In exercising his powers and performing his functions the Health Data Protection Ombudsman will act in an independent manner.

29 Removal of the Health Data Protection Ombudsman

The Health Data Protection Ombudsman may be removed from office by written notice issued by the Chairman or for reasons of inability, incapacity or misbehavior or for failure to properly discharge his duties and functions under this Regulation.

30 Resignation of the Health Data Protection Ombudsman

The Health Data Protection Ombudsman may at any time resign as the Health Data Protection Ombudsman by giving three (3) months written notice addressed to the Chairman.

31 Powers and Functions of the Health Data Protection Ombudsman

- (1) It is the duty of the Health Data Protection Ombudsman to promote good practices and, in particular, to perform his functions under this Regulation to promote the observance of the requirements of this Regulation.
- (2) The Health Data Protection Ombudsman has such powers, duties and functions as conferred on it under this Regulation and will exercise such powers and perform such functions in pursuit of the objectives of this Regulation.

-
- (3) Without limiting the generality of subsection (2), such powers, duties and functions of the Health Data Protection Ombudsman will include, so far as is reasonably practicable, to:
- (a) promote, by education and publicity, an understanding and acceptance of the Health Data Protection Principles and of the objects of those principles;
 - (b) investigate complaints relating to Interference with a Patient's Patient Health Information, and make recommendations to the Executive Committee and/or the Licensing Board with regard to any actions required to be undertaken;
 - (c) when requested to do so by a Licensee, conduct an audit of Patient Health Information maintained by that Licensee for the purpose of ascertaining whether or not the information is maintained according to the Health Data Protection Principles;
 - (d) monitor the use of Personal Identifiers, and to report to the Chairman from time to time on the results of that monitoring, including any recommendation relating to the need for, or desirability of taking, regulatory, administrative, or other action to give protection, or better protection, to the Patient or the Licensee;
 - (e) monitor compliance with the Health Data Protection Principles;
 - (f) examine and report to the Chairman on any proposed Regulation that makes provision for the:
 - (i) collection of Patient Health Information; or
 - (ii) use and/or disclosure of Patient Health Information;
 - (g) undertake educational programs on the Health Data Protection Ombudsman's own behalf or in cooperation with other persons or authorities acting on behalf of the Health Data Protection Ombudsman; for the purpose of promoting the protection of Patient Health Information;
 - (h) receive and invite representations from Patients and Licensees on any matter affecting Patient Health Information;
 - (i) provide advice (with or without a request) to the Chairman or a Licensee on any matter relevant to the operation of this Regulation and in particular to give protection or better protection to Patients with regard to their Patient Health Information;
 - (j) inquire generally into any matter, including any Regulation, or any practice, or procedure, or any technical development, if it appears to the Health Data Protection Ombudsman that there may be an Interference with Patient Health Information;
 - (k) undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments for Patients are minimized, and to report to the Chairman the results of such research and monitoring;
 - (l) report to the Chairman from time to time on the desirability of the acceptance, by DHCCA, of any international instrument such as those referred to in section 6(4), relating to Patient's Patient Health Information or personal information about an identifiable individual.

32 Production of Information

- (1) With regard to the Processing of Patient Health Information or a complaint about an Interference with Patient Health Information the Health Data Protection Ombudsman may require a Licensee by written notice to:
 - (a) give specified information; or
 - (b) produce specified documents,
- (2) The Licensee in respect of whom a requirement is made under subsection (1) must comply with that requirement. Where the Licensee fails to comply with the requirement, the Health Data Protection Ombudsman may impose a fine as determined by Rules, Policies and Standards approved by DHCCA from time to time.

33 Rules, Standards and Policies

- (1) After consultation with the Health Data Protection Ombudsman, DHCCA may make Rules, Standards and Policies in respect of:
 - (a) any matters related to the application of this Regulation; or
 - (b) as proposed by the Health Data Protection Ombudsman under subsection (2).
- (2) The Health Data Protection Ombudsman may propose Rules, Standards and Policies to the DHCCA in respect of any matter that facilitates the administration and application of this Regulation or furthers the purposes of this Regulation, including but not limited to:
 - (a) the development and publication of information to Licensees and their employees concerning the application and interpretation of this Regulation;
 - (b) procedures for initiating and filing complaints;
 - (c) fines;
 - (d) the conduct of the Health Data Protection Ombudsman and his employees and agents in relation to the exercise of powers and performance of functions.

34 Funding and fees

The Chairman will ensure that there is a provision of sufficient financial resources approved by DHCCA in respect of each financial year for the Health Data Protection Ombudsman to adequately perform his functions and exercise his powers in accordance with this Regulation.

35 Annual Funding of the Health Data Protection Ombudsman

- (1) The Health Data Protection Ombudsman will submit to the Chairman of the Board for approval estimates of the annual income and expenditure of the Health Data Protection Ombudsman for the next financial year.
- (2) Such estimates must include figures relating to levels of remuneration and entitlement to expenses of the Health Data Protection Ombudsman, employees and agents of the Health Data Protection Ombudsman.
- (3) The Health Data Protection Ombudsman must submit such estimates to the Chairman for approval not later than forty-five (45) days before the end of the current financial year.
- (4) The Chairman, in consultation with DHCCA, may accept or reject such estimates within forty-five (45) days of receiving them, in writing to the

Health Data Protection Ombudsman and where relevant state the reasons for rejection.

36 Accounts

- (1) The Health Data Protection Ombudsman must keep proper accounts of its financial activities.
- (2) The Health Data Protection Ombudsman must prepare financial statements for the previous financial year in accordance with accepted accounting standards before the end of the first quarter of the financial year.

37 Annual Report

- (1) As soon as practicable after 1 January in each year, the Health Data Protection Ombudsman must deliver to the Chairman a report on the management of the administrative affairs of the Health Data Protection Ombudsman for the previous year.
- (2) Such report shall give a true and fair view of the state of its operations in DHCC, and financial statements of the Health Data Protection Ombudsman, as at the end of the relevant financial year.

Part Six : Procedural provisions relating making a request to access and correction Patient Health Information

38 Patient Data Requests

- (1) This Part of this Regulation applies to the following requests, referred to as Patient Data Request:
 - (a) A request under principle 6(1)(a) to obtain confirmation of whether a Licensee holds Patient Health Information;
 - (b) A request under principle 6(1)(b) to be given access to Patient Health Information;
 - (c) A request made under principle 7(1) for correction of personal information.

39 Who may make requests?

- (1) Any Patient who has received Healthcare Services within DHCC may make a Patient Data Request.
- (2) A Representative may make a Patient Data Request on behalf of the Patient.

40 Form of request

A Patient Data Request must be made in writing.

41 No charge for Patient Data Requests

- (1) A Licensee will not require the payment, by or on behalf of any Patient who wishes to make a Patient Data Request under principle 6, of any charge in respect of the:
 - (a) provision of assistance; or
 - (b) making of the Patient Data Request to that agency; or
 - (c) transfer of the Patient Data Request to any other Licensee; or
 - (d) processing of the Patient Data Request, including deciding whether or not the Request is to be granted and, if so, in what manner.
- (2) A Licensee will not require the payment, by or on behalf of any Patient who wishes to make a Patient Data Request under principle 6 or principle 7, of a charge in respect of:
 - (a) the making available of information in compliance, in whole or in part, with the Patient Data Request;
 - (b) in the case of a Patient Data Request made under principle 7, the:
 - (i) correction of any information in compliance, in whole or in part, with the Patient Data Request; or
 - (ii) attaching, to any information, of a statement of any correction sought but not made.

42 Charges may be made for certain Patient Health Information

- (1) Section 41 does not apply to the provision of the actual photographs, x-ray films, scans, recordings and other such diagnostic procedures or similar type that has been obtained as the result of a diagnostic procedure.

-
- (2) In such cases the Licensee may charge for making available such information in accordance with DHCCA Policy.

43 Urgency

If a Patient or Representative making a Patient Data Request asks that the request is treated as urgent, the Patient or Representative must give reasons why the Patient Data Request should be treated as urgent.

44 Assistance

- (1) It is the duty of every Licensee to give reasonable assistance to a Patient or Representative, who has or intends to make a Patient Data Request, to
- (a) ensure the request is made in a manner that is in accordance with the requirements of this Regulation;
 - (b) to direct the request to the appropriate Licensee.

45 Transfer of requests

- (1) The Licensee to which the Patient Data Request is made shall promptly, and in any case not later than 10 working days after the day on which the request is received, transfer the request to the other Licensee and inform the Patient or Representative making the request accordingly where
- (a) a Patient Data Request is made to a Licensee or is transferred to a Licensee in accordance with this section; and
 - (b) The information to which the Patient Data Request relates:
 - (i) is not held by the Licensee but is believed by the person dealing with the request to be held by another Licensee; or
 - (ii) is believed by the person dealing with the request to be more closely connected with the functions or activities of another Licensee.

46 Decisions on requests

- (1) Subject to this Regulation, the Licensee to which a Patient Data Request is made or transferred will, as soon as reasonably practicable, and in any case not later than twenty (20) working days after the day on which the request is received by that Licensee:
- (a) decide whether the Patient Data Request is to be granted and, if it is to be granted, in what manner and, subject to sections 41 and 42, for what charge (if any); and
 - (b) give or post to the Patient who made the Patient Data Request notice of the decision on the request.
- (2) Where any charge is imposed, the Licensee may require the whole or part of the charge to be paid in advance.

47 Extension of time limits

- (1) Where an Patient Data Request is made or transferred to a Licensee, the Licensee may extend the time limit set out in section 45 or section 46 in respect of the request if the:
- (a) Patient Data Request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the Licensee; or

-
- (b) consultations necessary to make a decision on the Patient Data Request are such that a proper response to the request cannot reasonably be made within the original time limit.
 - (2) Any extension under subsection (1) must be for a reasonable period of time having regard to the circumstances.
 - (3) The extension shall be effected by giving or posting notice of the extension to the Patient who made the Patient Data Request, within twenty (20) working days after the day on which the request is received.
 - (4) The notice effecting the extension shall:
 - (a) specify the period of the extension; and
 - (b) give the reasons for the extension; and
 - (c) contain such other information as is necessary.

48 Form for making information available

- (1) Where the information in respect of which a Patient Data Request is made by any Patient is comprised in a Document, that information may be made available in one or more of the following ways:
 - (a) by giving the Patient a reasonable opportunity to inspect the Document; or
 - (b) by providing the Patient with a copy of the Document; or
 - (c) in the case of a Document that is an article or thing from which sounds or visual images are capable of being reproduced, by making arrangements for the Patient to hear or view those sounds or visual images; or
 - (d) in the case of a Document by which words are recorded in a manner in which they are capable of being reproduced in the form of sound or in which words are contained in the form of shorthand writing or in codified form, by providing the Patient with a written transcript of the words recorded or contained in the Document; or
 - (e) by giving an excerpt or summary of the contents; or
 - (f) by furnishing oral information about its contents.
- (2) Subject to section 49, the Licensee will make the information available in the way preferred by the Patient or Representative requesting it unless to do so would:
 - (a) impair efficient administration; or
 - (b) be contrary to any legal duty of the Licensee in respect of the document; or
 - (c) prejudice the interests protected by section 52.
- (3) Where the information is not provided in the way preferred by the Patient or the Representative requesting it, the Licensee shall give to that Patient or Representative the reason for not providing the information in that way and any grounds in support of that reason.

49 Deletion of information from Documents

- (1) Where the information in respect of which a Patient Data Request is made is comprised in a Document and there is good reason for withholding some of the information contained in that Document, the other information in that Document may be made available by making a copy of

that Document available with such deletions or alterations as are necessary.

- (2) Where a copy of a Document is made available under subsection (1), the Licensee shall give to the Patient or Representative:
- (a) the reason for withholding the information; and
 - (b) if the Patient or Representative so requests, the grounds in support of that reason.

50 Reason for refusal to be given

- (1) Where a Patient Data Request made by a Patient or Representative is refused, the Licensee shall give to the Patient:
- (a) the reason for not providing the information in that way and any grounds in support of that reason; and
 - (b) information concerning the Patient's right to make a complaint to the Health Data Protection Ombudsman.

51 Precautions before releasing Patient Health Information

- (1) Where a Patient Data Request is made under principle 6(1)(b), the Licensee will:
- (a) not give access to that information unless it is satisfied concerning the identity of the Patient or the Patient's Representative making the request; and
 - (b) ensure, by the adoption of appropriate procedures, that any information intended for a Patient is received:
 - (i) only by that Patient; or
 - (ii) where the Patient Data Request is made by the Patient's Representative, only by that Patient or his Representative;
 - (c) ensure that where the request is made by the Patient's Representative, the Representative has the written authority of that Patient to obtain the Patient Health Information or is otherwise properly authorized to obtain the Patient Health Information.

Part Seven : Good reasons for refusing access to Patient Health Information

52 Grounds for refusing access to Patient Health Information

- (1) A Licensee may refuse to disclose Patient Health Information requested under principle 6 if the disclosure of the information would be likely to:
 - (a) prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or
 - (b) endanger the safety of any individual; or
 - (c) involve the unwarranted disclosure of the affairs of another individual or of a deceased individual; or
 - (d) disclose a trade secret unless in the circumstances refusing to disclose is outweighed by other considerations which render it desirable, in the public interest, to make the information available; or
 - (e) unreasonably prejudice the commercial position of the person who supplied or who is the subject of the information.
- (2) A Licensee may refuse to disclose Patient Health Information under principle 6 if:
 - (a) after consultation undertaken (where practicable) by or on behalf of the Licensee, the Licensee is satisfied that the:
 - (i) Patient Health Information relates to that Patient; and
 - (ii) disclosure of the Patient Health Information (being information that relates to the physical or mental health of the Patient who requested it) would be likely to prejudice the physical or mental health of that Patient; or
 - (b) in the case of a Patient under the age of sixteen (16), the:
 - (i) disclosure of the Patient Health Information would be contrary to that Patient's interests; or
 - (ii) request is made by the Representative and it would be contrary to the Patient's interests for the Representative to be provided with the Patient Health Information and the Licensee has reasonable grounds for believing that the Patient does not or would not wish for the information to be disclosed;
 - (c) the disclosure of the Patient Health Information would constitute contempt of Court; or
 - (d) the request is frivolous or vexatious, or the Patient Health Information requested is trivial.
- (3) A Licensee may refuse a request made under principle 6 if the Patient Health Information requested:
 - (a) is not readily retrievable; or
 - (b) does not exist or cannot be found; or
 - (c) is not held by the Licensee and the person dealing with the request has no grounds for believing that the information is either:
 - (i) held by another Licensee; or

-
- (ii) connected more closely with the functions or activities of another Licensee.

Part Eight : Electronic Health Record

53 Establishment of an Electronic Health Record

DHCCA may establish an Electronic Health Record within DHCC in accordance with the provisions of this Regulation and in particular the Health Data Protection Principles.

54 Certain information from Electronic Health Record to be used for HIRAS

Where DHCCA establishes an Electronic Health Record under section 53, information may be extracted from that Electronic Health Record and held in HIRAS for the purposes set out in section 56.

55 HIRAS compliance with this Regulation

HIRAS must comply with the provisions of this Regulation and in particular the Health Data Protection Principles.

56 Purpose of HIRAS

- (1) HIRAS is an integrated electronic health network that will be a central data repository and data warehouse for Patient Health Information. The information may be used for:
 - (a) statistical analysis and the provision of reports;
 - (b) analysis to improve the quality and safety of Healthcare Services provided to Patients;
 - (c) ensuring the continuum of care between providers of Healthcare Services within DHCC;
 - (d) analysis of utilization of Healthcare Services provided within DHCC;
 - (e) a mechanism for Patients to access their Patient Health Information;
 - (f) research purposes subject to the requirements of the Research Council;
 - (g) education purposes subject to the requirements of the Academic Council.

57 Requirement to provide information

- (1) All Licensed Healthcare Operators will be required to:
 - (a) develop information systems that integrate into the Electronic Health Record; and
 - (b) provide Patient Health Information to the Electronic Health Record on a regular basis as set out in the Minimum Data Requirements Policy and any other applicable Policy, Standard or Rule.
- (2) Failure to comply with the requirement to provide Patient Health Information will be subject to the provisions Part Twelve of the Healthcare Operator Regulation.

58 Source of the Patient Health Information

Licensed Healthcare Operators on behalf of the Licensed Healthcare Professionals and Licensed Complementary and Alternative Medicine Providers will provide the Patient Health Information by electronic transmission.

59 Patient awareness

- (1) Licensed Healthcare Operators are responsible for:
 - (a) ensuring that Patients are made aware of the Electronic Health Records; and
 - (b) complying with the requirements of the Health Data Protection Principles and other requirements of this Regulation with regard to Electronic Health Records.

Part Nine : Transfer of Patient Health Information

60 Transfer of Patient Health Information out of DHCC

- (1) Patient Health Information may only be transferred to a third party located in a jurisdiction outside DHCC if:
- (a) an adequate level of protection for that Patient Health Information is ensured by the laws and regulations that are applicable to the third party; or
 - (b) Health Data Protection Ombudsman or his delegate has granted a permit or written authorization for the transfer and the Data Protection Officer applies adequate safeguards with respect to the protection of the Patient Health Information; or
 - (c) the Patient has authorized the proposed transfer; or
 - (d) the transfer is necessary for the ongoing provision of Healthcare Services to the Patient.

61 Meaning of adequate level of protection

A jurisdiction will be considered to have an adequate level of protection if that jurisdiction is listed as an acceptable jurisdiction under the DIFC Data Protection Regulation 2007, or has the written approval of the Health Data Protection Ombudsman.

Part Ten : Interference with a Patient's Patient Health Information

62 Interference with Patient Health Information

- (1) An action is an Interference with a Patient Health Information with regard to principles 1-5 and 8-12, if:
 - (a) the action breaches a Data Protection Principle; and
 - (b) in the opinion of the Health Data Protection Ombudsman the action has:
 - (i) caused loss, detriment, damage or injury to the Patient; or
 - (ii) adversely affected the rights, benefits, privileges, obligations or interests of the Patient; or
 - (iii) resulted in significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.
- (2) An action is an interference with a Patient's Patient Health Information with regard to principles 6 and 7, if the Licensee:
 - (a) refuses to make information available in response to a Patient Data Request; or
 - (b) refuses to correct information in response to a Patient Data Request, and
 - (c) the Health Data Protection Ombudsman considers that there is no proper basis for such refusal.

Part Eleven : Complaints

63 Complaints relating to an Interference with Patient Health Information

- (1) Every Licensee must designate a person or persons to deal with complaints alleging an Interference with Patient Health Information and facilitate the fair, simple, speedy, and efficient resolution of complaints.
- (2) Every Licensee must have a complaints procedure as provided by Part 8 of the Governing Regulation.

64 Complaints

A Patient or his Representative may make a complaint to the Health Data Protection Ombudsman alleging that an Action is or appears to be an Interference with a Patient's Patient Health Information.

65 Referral of complaint to the Executive Committee

- (1) On receipt of the complaint, the Health Data Protection Ombudsman, if the complaint has not already been investigated under the provisions of the Governing Regulation, will refer the matter to the Executive Committee to be investigated under the provisions of the Governing Regulation.
- (2) The Health Data Protection Ombudsman may only investigate an alleged complaint about Interference with Patient Health Information after the matter has been investigated in accordance with the Governing Regulation.

66 Referral of Complaint by Executive Committee

During its investigation process, the Executive Committee may at any time refer the matter directly to the Health Data Protection Ombudsman.

67 Complainant may refer the complaint to the Health Data Protection Ombudsman

If after the complaints investigation under the Governing Regulation the matter is still not resolved to the satisfaction of the Patient, the Patient may refer the complaint to the Health Data Protection Ombudsman for investigation.

68 Action on receipt of complaint

- (1) On receiving a complaint, the Health Data Protection Ombudsman may:
 - (a) investigate the complaint, or
 - (b) decide, in accordance with section 69, to take no action on the complaint.
- (2) The Health Data Protection Ombudsman must, within ten (10) working days, advise the complainant and the person to whom the complaint relates of the procedure that the Ombudsman proposes to adopt under subsection (1).

69 Health Data Protection Ombudsman may decide to take no action on complaint

- (1) The Health Data Protection Ombudsman may in his or her discretion decide to take no action or, as the case may require, no further action, on any complaint if, in the Ombudsman's opinion the:

-
- (a) length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable; or
 - (b) subject-matter of the complaint is trivial; or
 - (c) complaint is frivolous or vexatious or is not made in good faith; or
 - (d) individual alleged to be aggrieved does not desire that action be taken or, as the case may be, continued; or
 - (e) complainant does not have a sufficient personal interest in the subject-matter of the complaint; and
 - (f) the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.
- (2) Notwithstanding anything in subsection (1) of this section, the Health Data Protection Ombudsman may in his discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Ombudsman that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.
 - (3) In any case where the Health Data Protection Ombudsman decides to take no action, or no further action, on a complaint, the Ombudsman must inform the complainant of that decision and the reasons for it.

70 Proceedings of Health Data Protection Ombudsman

- (1) Before proceeding to investigate any matter under this Part of this Regulation, the Health Data Protection Ombudsman must:
 - (a) inform the person to whom the investigation relates, and any individual alleged to be aggrieved (if not the complainant), of the Ombudsman's intention to make the investigation; and
 - (b) inform the person to whom the investigation relates of the:
 - (i) details of the subject-matter of the investigation; and
 - (ii) right of that person to submit to the Ombudsman, within ten (10) working days, a written response in relation to the subject-matter of the investigation.

71 Settlement of complaints

Where it appears from a complaint, or any written response made in relation to a complaint under section 70, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Health Data Protection Ombudsman may, without investigating the complaint or, as the case may be, investigating the complaint further, use his best endeavors to secure such a settlement and assurance.

72 Parties to be informed of result of investigation

Where any investigation is made following a complaint, the Health Data Protection Ombudsman must conduct the investigation with due expedition and must inform the parties concerned, within ten (10) working days after the conclusion of the investigation and in such manner as the Ombudsman thinks proper, of the result of the investigation and of what further action (if any) the Ombudsman proposes to take in respect of that complaint.

73 Procedure after investigation

- (1) Where the Health Data Protection Ombudsman, after making any investigation under this Part of this Regulation, is of the opinion:
 - (a) in the case of a complaint, that the complaint has substance, the Health Data Protection Ombudsman must use his best endeavors to secure a settlement between any parties concerned and, if the Ombudsman considers it appropriate, a satisfactory assurance against the repetition of any action that was the subject-matter of the investigation or the doing of further actions of a similar kind by the person concerned; or
 - (b) in any other case, that the matter ought to be proceeded with, the Health Data Protection Ombudsman must use his best endeavors to secure such an assurance as is referred to in sub section 1(a).
- (2) The Health Data Protection Ombudsman may refer the matter to the Executive Committee for the purpose of deciding whether to refer the matter to the Licensing Board if:
 - (a) In the circumstances referred to in section 71, the Health Data Protection Ombudsman is unable to secure such a settlement and assurance as is referred to in that section; or
 - (b) In the circumstances referred to in sub section 1(a) or 1(b), the Health Data Protection Ombudsman is unable to secure such a settlement and assurance or, as the case may be, such an assurance as is referred to in either of those subsections; or
 - (c) In any case to which section 71 or subsection (1) of this section applies, it appears that the action that was the subject-matter of the investigation was done in contravention of such an assurance as is referred to in that section or that subsection, given on a previous occasion, or that any term of such a settlement as is referred to in that section or that subsection, reached on a previous occasion, has not been complied with.

74 Health Data Protection Ombudsman to report Licensee not meeting the Regulation requirements

- (1) The Health Data Protection Ombudsman must refer the matter to the Licensing Board and notify the Executive Committee of the referral If, during or after any investigation, the Health Data Protection Ombudsman is of the opinion that there is evidence of a:
 - (a) Licensed Healthcare Professional or Licensed Complementary and Alternative Medicine Provider not meeting the Required Standard of Competence as defined in the Healthcare Professionals Regulation and the Complementary and Alternative Medicine Regulation; or
 - (b) Licensed Healthcare Operator not meeting the requirements of the Healthcare Operators Regulation.

75 Compliance with requirements of Health Data Protection Ombudsman

- (1) This section applies in every case where, during the course of an investigation the Health Data Protection Ombudsman requires that a Licensee provides any information or Document or thing which relates to that investigation.
- (2) The Licensee to which the requirement is made must as soon as reasonably practicable, and in no case later than twenty (20) working days

after the day on which the requirement is received by the Licensee, comply with the requirement.