
ICD-10 National Task Team

**Patient Confidentiality
Subcommittee Report**

2007

ACKNOWLEDGEMENTS

The implementation of ICD-10 codes in South Africa cannot be complete without addressing the important issue of patient confidentiality. With this in mind, the National ICD-10 Task Team set up a dedicated subcommittee to address this issue. The activities of this subcommittee were conducted through an open and transparent process.

The relevant stakeholders met regularly over the past eight months and I would like to acknowledge the many individuals who gave generously of their time, both in meetings and in preparation of work outside of formal meetings. I would also like to acknowledge the various organisations who hosted the subcommittee meetings. I would also like to thank the various Statutory Bodies for their participation in this subcommittee.

A special thank you goes to Karen Dreyer of MediKredit for her effort and input beyond the normal levels of participation. I would also like to note the support and guidance of Patrick Matshidze from the Council of Medical Schemes and Dr S Khotu from the Department of Health.

Finally, I would like to thank everyone who made a concerted effort to finalise this report in the shortest time possible in order to give guidance to the South African health care industry as related to this sensitive and important topic.

Dr BH Modi
3 May 2007

TABLE OF CONTENTS

I.	EXECUTIVE SUMMARY	6
II.	PARTICIPANTS	9
III.	ABBREVIATIONS	10
IV.	DEFINITIONS	11
V.	BACKGROUND.....	15
VI.	TERMS OF REFERENCE	18
VII.	OBJECTIVES.....	19
VIII.	FLOW OF PERSONAL HEALTH INFORMATION.....	20
IX.	REGULATORY REVIEW	21
A.	Constitution of the RSA, No. 108 of 1996.....	21
B.	Allied Health Professions Act, No. 63 of 1982 & Regulations issued by Allied Health Professions Council of South Africa (“AHPCSA”).....	22
C.	Children’s Act, No. 38 of 2005.....	24
D.	Choice on Termination of Pregnancy Act, No. 92 of 1996	25
E.	Electronic Communications and Transactions Act, No 25 of 2002 (“ECT Act”).....	26
F.	Health Act, No. 63 of 1977.....	29
G.	Health Professions’ Act, No. 56 of 1974 & Regulations (“HPA”) and Ethical Rules of the HPCSA.....	30
H.	Medical Schemes Act No. 131 of 1998 and Regulations thereto, as amended (“the MSA”)	33
I.	Mental Health Care Act, No. 17 of 2002.....	35
J.	National Health Act, No. 61 of 2003 (“the NHA”)	37
K.	Nursing Act, No. 50 of 1978 (“the Current Nursing Act”), Nursing Act, No. 33 of 2005 (“the New Nursing Act”) and Rules issued by the South African Nursing Council (“SANC”).....	40

L.	Pharmacy Act, No. 53 of 1974 & Regulations and Ethical Rules issued by the South African Pharmacy Council (“SAPC”)	42
M.	Promotion of Access to Information Act, No. 2 of 2000 (“PAIA”).....	43
N.	Protection of Personal Information Bill.....	44
O.	Sterilisation Act, No. 44 of 1998 and regulations published under Government Notice R872 on 16 July 1999.....	49
P.	Traditional Health Practitioners Act 35 of 2004	50
Q.	Patients’ Rights Charter.....	51
X.	INFORMED CONSENT FOR SUBMISSION OF PERSONAL HEALTH INFORMATION	52
XI.	INFORMATION SECURITY	55
XII.	PROTECTION OF PERSONAL HEALTH INFORMATION WITHIN DATA MANAGEMENT COMPANIES.....	59
XIII.	RECOMMENDATIONS	60
	1. Introduction	60
	2. General Recommendations.....	60
	3. Health Care Provider Specific Recommendations.....	62
	4. Medical Scheme, Medical Scheme Administrator and Managed Care Organisation Specific Recommendations.....	62
	5. Professional Council Specific Recommendations.....	63
	6. Council for Medical Scheme Specific Recommendations	63
XIV.	CONCLUSION	65
XV.	ANNEXURES	66
	ANNEXURE A: Pro Forma Informed Consent for Health Care Providers.....	66
	ANNEXURE B: ISO and SABS Standards relevant to the Implementation of ICD-10 and other Codes as the South African National Standard for Diagnosis Coding	67
	ANNEXURE C: Comments on ISO/DIS 27799: Health Informatics – Security Management in Health using ISO/IEC 17799.....	68
	ANNEXURE D: Comments on ISO 22857: Health Informatics – Guidelines on Data Protection to Facilitate Trans-Border Flows of Personal Health Information.....	70

ANNEXURE E: Code of Conduct for Data Management Companies as proposed by Members of the South African Health Care Data Management Society..... 71

ANNEXURE F: Mission Statement of Data Management Companies as proposed by Members of the South African Health Care Data Management Society..... 72

I. EXECUTIVE SUMMARY

1. ICD-10 is a diagnosis coding standard that was adopted by the **National Health Information System of South Africa (NHISSA)**, and currently serves as the diagnosis coding standard of choice for both the Public and the Private Health Sectors in South Africa.
2. The rationale for the implementation of ICD-10 is four-fold:
 - 2.1. There is a need to **standardise the health data collection** process in South Africa
 - 2.2. Regulation 5(f) of the MSA prescribes the **manner of submission of claims** for health services rendered
 - 2.3. There is a need to **facilitate an efficient reimbursement system**, for providers that is consistent with legislation and **improves the risk management practices** by medical schemes
 - 2.4. The MSA caters for a **minimum set of guaranteed benefits** to be covered by medical schemes. Entitlement to these benefits is diagnosis-driven and is appropriately identified using ICD-10
3. Prior to 2005, health service providers supplied health related information on claims, in the form of procedure and other codes, to medical schemes. In addition, a patient's diagnosis information was often provided in explicit, descriptive text on claims/referral notes. Despite this practice, the issue of patient confidentiality only came to the fore with the implementation of ICD-10 coding in 2005.
4. To resolve these patient confidentiality issues, the National ICD-10 Task Team formed the **Patient Confidentiality Subcommittee** in March 2006. Participants included representatives from the National Department of Health, the Council of Medical Schemes, members of the various Statutory Councils (such as the Health Professions Council of South Africa and the SA Pharmacy Council), the South African Law Commission and other parties representing health care providers, medical schemes, data management companies and consumers. The subcommittee was mandated to identify and find possible solutions to confidentiality issues as it relates to personal health information.
5. The following key confidentiality issues were identified by the participants:
 - 5.1. Legally, **informed consent** is required from patients prior to the disclosure of any personal health information to any party, including secondary providers (e.g. radiologists and pathologists) and medical schemes. The current practice of providing blanket consent for disclosure of health information to the medical scheme and other related parties, when signing a medical scheme contract, is inadequate.
 - 5.2. An **ethical ruling within the HPCSA** prohibited any health care provider who was an HPCSA member from divulging health related information to a non-HPCSA

health provider (e.g. pharmacists). This ruling was in conflict with the Medical Schemes Act which required the release of such clinical information to other members of the health care team and to medical schemes.

5.3. **Data management companies** do not fall under any regulatory body at present. This raised concerns about their confidentiality and security standards.

6. To resolve these issues a **regulatory review** had to be undertaken to establish whether adequate safeguards were in place and several consultative meetings were held by the subcommittee. The main outcomes of these meetings were the following:

6.1. This report and its recommendations were drafted to document a framework for the submission, transmission and storage of all **Personal Health Information** in all relevant forms in a confidential and secure manner;

6.2. It is to be noted that ICD-10 coding is only one type of Personal Health Information. **Other coding types such as NAPPI and CCSA** also constitute Personal Health Information;

6.3. Regulation 5(f) of the Medical Schemes Act of 1998 requires that all accounts by suppliers of services contain the **relevant diagnostic and other item code numbers** that relate to the health service provided;

6.4. As required by law, the **privacy, confidentiality, security and integrity** of personal health information must be maintained by all recipients thereof;

6.5. In keeping with both legal and ethical rule requirements in SA, **health care providers must obtain written informed consent** from the patient or other legally authorised person for the disclosure of any personal health information (e.g. ICD-10 codes) to medical schemes and other members of the health services team treating the patient;

6.6. Informed consent requires that the **purpose, intended recipients, likely consequences of disclosure and consequences of non-disclosure** (e.g. the medical scheme may elect not to reimburse the claim of the patient) be given to the patient;

6.7. **Medical scheme contracts or application forms** used for beneficiaries should also state the reasons, the likely consequences of disclosure as well as non-disclosure and the intended recipients of personal health information;

6.8. The Registrar of the HPCSA agrees that in order to **maintain continuity of care, diagnosis and procedure information needs to be shared amongst members of the health services team across all Professional Councils**, provided that privacy, confidentiality, security and integrity of this information is maintained at all times;

6.9. **Data management companies** (i.e. companies that switch or process data) that are members of the South African Health Care Data Management Society have agreed to sign and abide by a Code of Conduct and Mission Statement

for the protection of personal health information in the absence of a regulatory body that oversees the activities of these companies. All data management companies are also encouraged to adopt the principles of Chapter 8 of the Electronic Communications and Transactions Act, No 25 of 2002;

- 6.10. In order to provide guidance on the issue of informed consent for the disclosure of personal health information, the subcommittee has drawn up a **proposed generic informed consent document** that may be used as a basis for reference by the respective Professional Councils who in their discretion should adapt this proposed consent to cater for the needs of the respective health care providers in line with applicable legislation and ethical rulings pertaining to such health care providers. This proposed generic informed consent contains the minimum amount of information that must be given to patients and may be modified to include any extra information a health care provider may require.
- 6.11. It is to be noted that **patient confidentiality and information security are legal obligations**.
- 6.12. Although there is an **adequate regulatory framework** in place to protect personal health information, **further recommendations** have also been suggested by the subcommittee to **improve the level of compliance** towards maintaining the privacy, confidentiality, security and integrity of personal health information across the data chain / information pathway comprising of health care providers, medical schemes, medical scheme administrators, managed care organisations, brokers, data management companies and any other related third parties.
- 6.13. Until the Protection of Personal Information Bill is promulgated, it is recommended that health care providers and medical schemes conclude **written agreements with third party service providers** to ensure that personal health information is protected.

II. PARTICIPANTS

The following organisations are currently participating in this subcommittee:

1. Board of Healthcare Funders (BHF)
2. Community Health Group
3. Council for Medical Schemes (CMS)
4. Department of Health (DoH)
5. Health Professions Council of South Africa (HPCSA)
6. Managed Healthcare Systems Ubuntu (MHS Ubuntu)
7. Medical Protection Society (MPS)
8. MediKredit Integrated Healthcare Solutions (Pty) Ltd
9. Netcare
10. Patient Health Alliance of Non-Governmental Organisations (PHANGO)
11. Pharmaceutical Society of South Africa (PSSA)
12. Private Healthcare Information Standards Committee (PHISC)
13. South African Law Reform Commission
14. South African Managed Care Coalition (SAMCC)
15. South African Medical Association (SAMA)
16. South African Nursing Council (SANC)
17. South African Pharmacy Council (SAPC)
18. Synaxon (Pty) Ltd

III. ABBREVIATIONS

1. **AHPCSA:** Allied Health Professions Act, No. 63 of 1982 & Regulations issued by Allied Health Professions Council of South Africa.
2. **CCSA:** Complete Current Procedural Terminology (CPT) system for South Africa
3. **CMS:** Council for Medical Schemes.
4. **ECT Act:** Electronic Communications and Transactions Act, No. 25 of 2002.
5. **HPA:** Health Professions Act, No. 56 of 1974.
6. **HPCSA:** Health Professions Council of South Africa.
7. **MSA:** Medical Schemes Act, No. 131 of 1998 and Regulations thereto, as amended.
8. **NAPPI:** National Pharmaceutical Product Interface code
9. **NHA:** National Health Act, No. 61 of 2003.
10. **NHISSA:** National Health Information System of South Africa.
11. **PAIA:** Promotion of Access to Information Act, No. 2 of 2000.
12. **REF:** Risk Equalisation Fund.
13. **SAPC:** South African Pharmacy Council
14. **SANC:** South African Nursing Council.
15. **WHO:** World Health Organisation.

IV. DEFINITIONS

1. Confidentiality

The prevention of disclosure of PHI to other than authorised individuals or entities.

2. Data Subject

The person to whom personal information relates.¹

The ECT Act defines a “data subject” as any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored.

For purposes of this report, a patient constitutes a data subject.

3. Data Controller

The ECT Act defines a “data controller” as any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.

For purposes of this report, health care providers, medical schemes, medical scheme administrators, managed care organisations, data management companies, the Road Accident Fund, the Compensation Commissioner (COIDA), the Life Offices’ Association of South Africa (LOA), and any other entity switching or processing PHI electronically are considered to be data controllers.

4. Data Management Company

Switching companies, data management companies, data transfer companies, pharmaceutical benefit management companies and any other entity switching or processing personal health information but excluding any entity that is accredited by the CMS.

5. Health Care Provider²

Means a person providing health services in terms of any law, including in terms of the-

5.1. Allied Health Professions Act, 1982 (Act No. 63 of 1982);

5.2. Health Professions Act, 1974 (Act No. 56 of 1974);

5.3. Nursing Act, 1978 (Act No. 50 of 1978);

¹ Definition as per the Protection of Personal Information Bill

² Definition as per NHA

- 5.4. Pharmacy Act, 1974 (Act No. 53 of 1974); and
- 5.5. Dental Technicians Act, 1979 (Act No. 19 of 1979).

6. **Health Services³**

- 6.1. health care services, including reproductive health care and emergency medical treatment, contemplated in section 27 of the Constitution;
- 6.2. basic nutrition and basic health care services contemplated in section 28(1)(c) of the Constitution;
- 6.3. medical treatment contemplated in section 35(2)(e) of the Constitution; and
- 6.4. municipal health services.

7. **Health Services Team**

The team who comprise of the people providing health services for each patient and the administrative staff who directly support those services.

8. **Health Establishment⁴**

The whole or part of a public or private institution, facility, building or place, whether for profit or not, that is operated or designed to provide inpatient or outpatient treatment, diagnostic or therapeutic interventions, nursing, rehabilitative, palliative, convalescent, preventative or other health services.

9. **ICD-10**

International Statistical Classification of Diseases and Related Health Problems – Tenth Revision as published by the WHO.

10. **Identifiable Person**

One who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

11. **Patient**

Recipient / subject of health services.

12. **Personal Health Information (PHI)**

Information about an identifiable, natural person that relates to the physical or mental health, well-being or disability of the individual, or to provision of health services to the individual⁵. Such information may include:

³ Definition as per NHA

⁴ Definition as per NHA

- 12.1. information about the registration of the individual for the provision of health services;
- 12.2. information about payments or eligibility for health care in respect to the individual;
- 12.3. a number or symbol assigned to an individual to uniquely identify the individual for health purposes;
- 12.4. any information about the individual that is collected in the course of the provision of health services to the individual, including ICD-10 codes, NAPPI and any other codes;
- 12.5. information derived from the testing or examination of a body part or bodily substance; and
- 12.6. identification of a person (e.g. a health care provider which renders health services to the individual).

NOTE: PHI does not include information that, either by itself or when combined with other information available to the holder, is anonymised, i.e. the identity of the individual who is the subject of the information cannot be ascertained from the information.

13. **Privacy**

In its simplest form, privacy is concerned with access to PHI for purposes of this report.

The definition of "privacy" as set out in the Appeal Court case of *National Media v Jooste* (1996 3 SA 262) and referred to in the Constitutional Court case of *Harold Bernstein and Others v L. Von Wielligh Bester NO and Others*(CCT23/95) and other High Court cases reads as follows:

"Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private."

14. **Processor**

The person or body which processes personal information for the responsible party, without coming under the direct authority of that party.⁶

For purposes of this report, health care providers, medical schemes, medical scheme administrators, managed care organisations, data management companies, the Road Accident Fund (RAF), the Compensation Commissioner (COIDA), the Life Offices' Association of South Africa (LOA) and any other entity switching or processing PHI are considered to be processors.

15. **Professional Councils**

Refers to Councils such as the AHPCSA, the HPCSA, the SANC and the SAPC.

⁵ PAIA, the ECT Act and the Protection of Personal Information Bill have corresponding definitions for PHI.

⁶ Definition as per the Protection of Personal Information Bill

16. **Quality of Health Services**

The degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge.⁷

Quality is a comprehensive and multifaceted concept. Experts generally recognise several distinct dimensions of quality that vary in importance depending on the context:

- 16.1. technical competence;
- 16.2. access to services;
- 16.3. effectiveness;
- 16.4. interpersonal relations;
- 16.5. efficiency;
- 16.6. continuity;
- 16.7. safety;
- 16.8. amenities (resources).

17. **Responsible Party**

The natural person, juristic person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information both electronically and manually.⁸

For purposes of this report, any of the following parties will constitute a “responsible party” if such a party is the recipient of PHI (for example an ICD-10 code linked to an identifiable patient):

- health care providers;
- a medical scheme;
- the CMS;
- the REF (once legislated); and/or
- the Department of Health / State.

18. **Security**

Preservation of confidentiality, integrity (including authenticity, accountability and auditability) and the availability of information.

⁷ USAID, 1999

⁸ Definition as per the Protection of Personal Information Bill

V. BACKGROUND

1. Despite the fact that health care providers and health establishments have been submitting various claims and procedure codes relating to a patient encounter to medical schemes for reimbursement for many years, the issue of patient confidentiality came to the fore with the official implementation of ICD-10 coding in June 2005 by the CMS in accordance with **section 59 and regulation 5 of the MSA**.
2. ICD-10 coding is a diagnostic coding standard that was adopted by the **National Health Information System of South Africa** (NHISSA), and forms part of the health information strategy of the Department of Health, outlined in the White Paper on the Transformation of the Health System of 1996. It is the diagnostic coding standard that is accepted by all role-players in the health care industry as the **coding standard of choice** in the **public** as well as **private sector**.
3. ICD-10 codes are clinical diagnostic codes that **translate** the written description of medical and health information into codes in a **standardised format**, e.g. J03.9 is an ICD-10 code for acute tonsillitis unspecified.
4. ICD-10 coding is important for **medical scheme beneficiaries** in that it assists them in the following ways:
 - 4.1. Enabling **patient access** to health care;
 - 4.2. A beneficiary's medical scheme entitlements are based on conditions covered in the **particular benefit option** that the main member would have chosen. Such a benefit option contains a **basket of services** that often has limits on the health services that will be paid for. Reimbursement for the relevant health services is then linked to the diagnosis and procedures that the health care provider renders to the beneficiary. The medical scheme is able to **efficiently effect reimbursement** for such services only if it receives details pertaining to the type of service that the beneficiary received, as contained in the diagnosis code or such other codes as may be appropriate. Failure to disclose such information would make it impossible for the medical scheme to assign benefits appropriately and to determine to what extent the benefits should be covered⁹. As a result, a beneficiary might forfeit his or her entitlements as per the Prescribed Minimum Benefits regulations of the MSA, as the Prescribed Minimum Benefit services might be paid from the wrong benefit (e.g. medical savings account) or it might not be paid at all if the day-to-day or hospital benefit limits of the beneficiary have been exceeded.
5. ICD-10 coding is important for the **South African health care industry** in that it lends itself well to:
 - 5.1. **Improvement of efficiency of health care** through easy storage, retrieval and analysis of information for patient care, research, performance improvement, health care planning and facility management;
 - 5.2. Enabling **fair reimbursement** for health services provided;

⁹ Sections 29 and 59 and Regulation 5 of the MSA

- 5.3. **Communicating in a predictable, consistent and reproducible manner;**
 - 5.4. Enabling **reliable communication** about health care data among many participants in the health care industry in a **standardised manner;**
 - 5.5. Facilitating **efficient payment** of claims from health care providers and improve clinical and financial risk management practices by medical schemes;
 - 5.6. Enable **successful implementation of the Risk Equalisation Fund** in order to minimise the clinical and financial risk of each individual medical scheme;
 - 5.7. Enabling South Africa as a member of the WHO to **submit health data as required by the WHO.**
6. Therefore, it is important that personal health information such as ICD-10 codes be shared with other health care providers that comprise of the health services team of the patient to ensure **quality and continuity of health services.**
 7. For the successful implementation of ICD-10 coding, the health care provider has to submit:
 - 7.1. the patient diagnosis as an ICD-10 code on their **accounts** to the medical scheme;
 - 7.2. the ICD-10 codes when **referring** the patient to other health care providers for additional services, such as to radiologists, pathologists and pharmacists. Some radiologists, pathologists, pharmacists and other health care providers are not able to make a diagnosis. Therefore, they require the diagnosis information from the referring doctor;
 - 7.3. the ICD-10 codes on **health establishment discharge reports** (if applicable).
 8. Health care providers and health establishments are concerned about the notion of releasing these clinically specific details of the patient encounter, regardless of the reason, to others.
 9. A dilemma existed between the **Ethical Rulings of certain Professional Councils** in respect of keeping all clinically related information concerning a patient private and confidential versus the statutory obligations to release such clinical information in the form of ICD-10 codes.
 10. In order to resolve much of the uncertainty surrounding patient confidentiality in relation to *inter alia* ICD-10 codes, the National ICD-10 Task Team formed the **Patient Confidentiality Subcommittee** in March 2006, under the chairmanship of Dr BH Modi.

11. Although the submission of ICD-10 codes initiated this consultative process, it is to be noted that such coding is only one type of personal health information. Other coding types such as NAPPI¹⁰ and CCSA¹¹ also constitute personal health information. Furthermore, other personal health information may reside as part of clinical notes, health records, claims, accounts etc. This report and its recommendations were therefore drafted to document **a framework for the submission, transmission and storage of all personal health information in all relevant forms in a confidential and secure manner.**

¹⁰ NAPPI means the National Pharmaceutical Product Interface code being a unique product identifier for surgical products, medical appliances and consumables, pharmaceutical and other medicinal products as allocated by MediKredit Integrated Healthcare Solutions (Pty) Ltd.

¹¹ CCSA means the Complete Current Procedural Terminology (CPT) system for South Africa based on original CPT codes, together with South African specific codes.

VI. TERMS OF REFERENCE

The Patient Confidentiality Subcommittee has been tasked by the National ICD-10 Implementation Task Team to document a framework, which will assure health care providers that, by documenting personal health information such as ICD-10 and any other codes as legally required, personal health information will be secure and kept confidential in the public as well as private health care sectors.

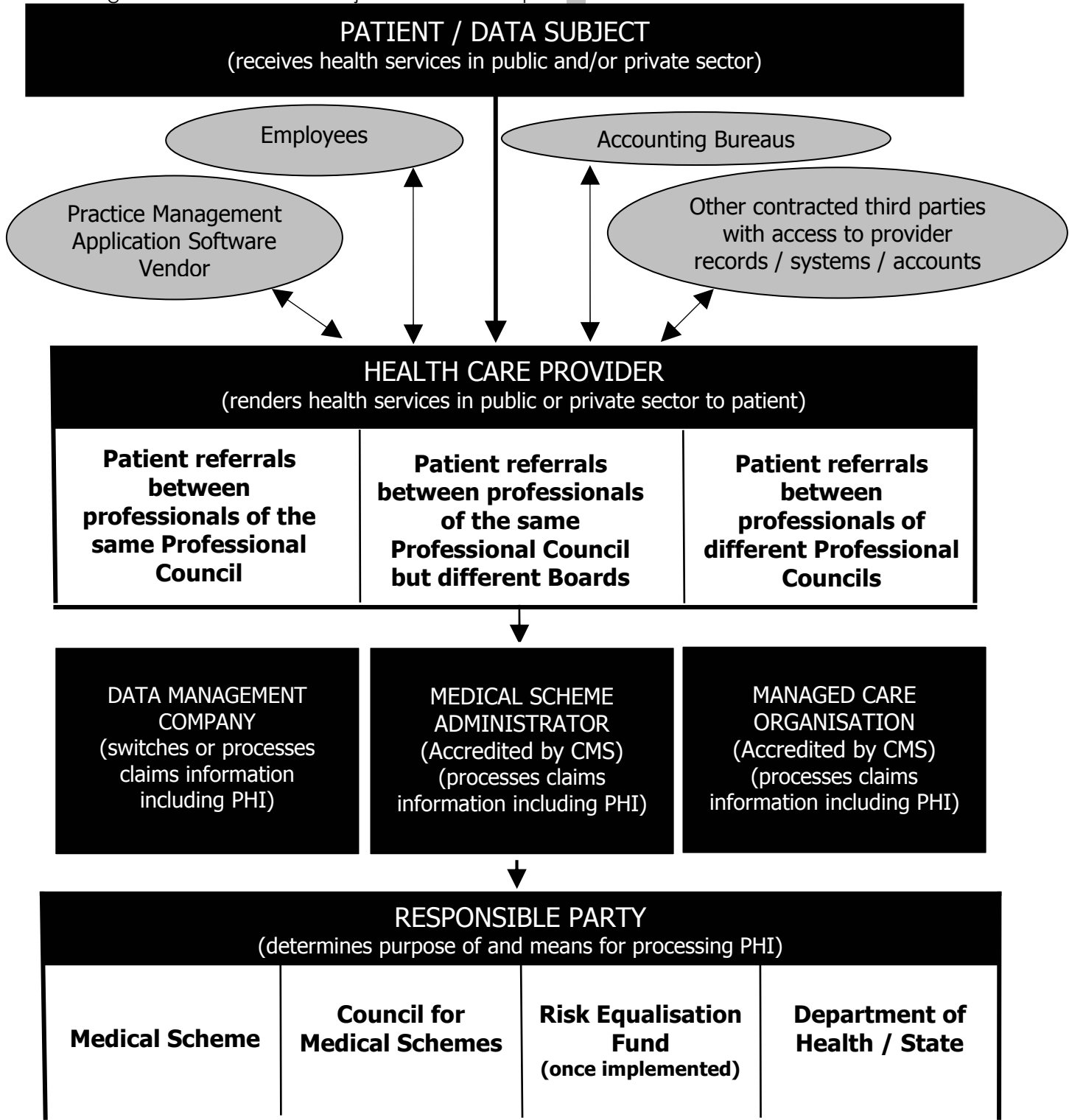
VII. OBJECTIVES

1. To review the existing regulatory framework to establish whether there are adequate safeguards in place to maintain the privacy, confidentiality, security and integrity of personal health information across the data chain / information pathway comprising of health care providers, medical schemes, medical scheme administrators, managed care organisations, brokers, data management companies and any other related third parties.
2. To identify the manner in which informed consent to disclosure of personal health information should be obtained from patients.
3. To clearly define the purpose and consequences of disclosure and non-disclosure of personal health information.
4. To review the disclosure of personal health information to other health care providers of:
 - 4.1. the same Professional Council and the same Professional Board (e.g. GP – ENT);
 - 4.2. the same Professional Council but different Professional Boards (e.g. GP – physiotherapist);
 - 4.3. other Professional Councils (e.g. GP – pharmacist); or
 - 4.4. the same health establishment;

to ensure quality and continuity of health services in respect of the patient.

VIII. FLOW OF PERSONAL HEALTH INFORMATION

In order to fully understand the complexity of the confidentiality issue with regard to PHI, it is necessary to draw attention to the flow of PHI within the health care environment. The diagram below illustrates the flow of identifiable patient data / PHI amongst role players in the health care industry and highlights the various parties who may have access to such data. This diagram must be read in conjunction with Chapter VI above.



IX. REGULATORY REVIEW

This Chapter details the pertinent provisions of current legislation, ethical rules, acts still to be proclaimed and bills as they relate to the protection of PHI to establish whether there are adequate regulatory safeguards in place to maintain the privacy, confidentiality, security and integrity of PHI.

The legislation quoted in this Chapter caters for **contravention** of the provisions thereof. Offences are clearly defined and persons / entities when convicted of an offence may *inter alia* be liable on conviction to a **fine, imprisonment or both**.

Contravention of Ethical Rules as quoted in this Chapter may result in **disciplinary action** being taken against the individual.

A. Constitution of the RSA, No. 108 of 1996

1. The **pertinent human rights** applicable to the disclosure of PHI are:
 - 1.1. the right to **equality** (Section 9);
 - 1.2. **privacy** and **data protection** (Section 14); and
 - 1.3. the right of **access to information** (Section 32).
2. In constitutional law, every person has the right to privacy, which includes the right to have his or her information kept confidential. No distinction is made between minor or adults in this regard. It is therefore imperative that a health care provider must ensure at all times that appropriate action is taken to protect the privacy of all patients, including minors.
3. As no right is absolute, section 36 of the Constitution provides for the **limitation of rights** by "law of general application", to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. To evaluate whether the limitation (or in this case *breach / infringement*) of the right to confidentiality is justifiable or not, all relevant factors must be taken into account, such as:
 - 3.1. the nature of the right (i.e. the right to privacy in the health care context);
 - 3.2. the importance of the purpose of the limitation (for example ICD-10 legislative requirement);
 - 3.3. the nature and extent of the limitation (i.e. impact on all concerned);
 - 3.4. the relation between the limitation and its purpose (for example, does ICD-10 achieve stated objective?); and
 - 3.5. less restrictive means to achieve the purpose.
4. As laws and their implementation can be subjected to constitutional scrutiny, the **objectives of disclosure** of PHI must be clear.

B. **Allied Health Professions Act, No. 63 of 1982 & Regulations issued by Allied Health Professions Council of South Africa (“AHPCSA”)**

1. The following are considered Allied Health Professions:
 - 1.1. Ayurveda:
 - 1.1.1. Ayurveda doctor;
 - 1.1.2. Panchakarma technician;
 - 1.1.3. Primary health care advisor;
 - 1.1.4. Yoga therapists;
 - 1.2. Chinese medicine and acupuncture:
 - 1.2.1. Doctor of Chinese medicine;
 - 1.2.2. Acupuncturist;
 - 1.3. Chiropractic;
 - 1.4. Homeopathy;
 - 1.5. Naturopathy;
 - 1.6. Osteopathy;
 - 1.7. Phytotherapy;
 - 1.8. Therapeutic aromatherapy;
 - 1.9. Therapeutic massage therapy; and
 - 1.10. Therapeutic reflexology.
2. A practitioner in terms of this Act may, *inter alia*, **diagnose and prescribe and dispense** medicine. This is however not the case as far as therapists in terms of the Act are concerned.¹²
3. A **practitioner** is a person registered as an acupuncturist, ayurveda practitioner, chiropractor, homeopath, naturopath, osteopath or phytotherapist; and a **therapist** is a person registered as a therapeutic aromatherapist, therapeutic massage therapist or therapeutic reflexologist.¹³
4. There is **no duty of confidentiality** placed on practitioners or therapists in terms of the Act in respect of patient information.
5. This Act provides that the AHPCSA shall, after consultation with the relevant professional board established in terms of the Act (“the professional board”) on the approval of the Minister of Health, by notice in the *Gazette* **specify the acts or omissions** in respect of which the AHPCSA or professional board, may take **disciplinary steps** under Chapter 3 of the Act, provided that the powers of the AHPCSA or the relevant professional board to inquire into and deal with any complaint, charge or allegation, shall not be limited to the acts or omissions so specified.¹⁴

¹² Section 1(2) of the Act and section 16(4).

¹³ Section 1 of the Act.

¹⁴ Section 29 of the Act.

6. The disclosure by a practitioner of **any information concerning a patient** obtained in the course of the professional activities of the practitioner, shall constitute an act in respect of which the AHPCSA may take **disciplinary steps** - provided that this rule shall not be applicable if such information is made known with the explicit consent of the patient or, in the case of a minor, with the consent of the parent or guardian, or where instructed thereto by a court of law or where a practitioner is otherwise legally compelled to do so, or where such disclosure is in the explicit interest of the patient who is not able to or who is unfit to grant permission himself.¹⁵
7. The provisions of the above rules may have to be revised once the **Children's Act** has been promulgated insofar as these rules relate to consent of the parent or guardian as opposed to consent by the minor.

¹⁵ Rule 11 of the Schedule published under Government Notice R 1746 of August 1983.

C. Children's Act, No. 38 of 2005¹⁶

1. A “**child**” for purposes of this Act means a person under the age of 18 years.
2. The rights which a child has in terms of this Act supplement the rights which a child has in terms of the **Bill of Rights**.¹⁷
3. Every child has the right to confidentiality regarding his or her health status **except when maintaining such confidentiality is not in the best interests of the child**.¹⁸ Furthermore, the results of a **virginity test** may not be disclosed without the consent of the child.¹⁹
4. A child may approach a Court if his / her rights in terms of the Bill of Rights or this Act has been infringed or threatened and the **Court may grant appropriate relief**, including a declaration of rights.²⁰
5. No person may disclose the fact that a child is **HIV positive** without consent given by:
 - 5.1. the child, if the child is 12 years or older; or
 - 5.2. the child if, the child is under the age of 12 years and is of sufficient maturity to understand the benefits, risks and social implications of such a disclosure; or
 - 5.3. the parent or care-giver, if the child is under the age of 12 years and is not of sufficient maturity to understand the benefits, risks and social implications of such a disclosure; or
 - 5.4. such other entities as provided for in section 133(2).
6. A child is entitled to confidentiality if he / she obtain **condoms, contraceptives or contraceptive advice** in terms of this Act.
7. Once this Act has been promulgated, certain **Ethical Rules** relating to the procurement of informed consent as established by the respective Professional Councils or Professional Boards of Councils may have to be reviewed.

¹⁶ Please note that this Act has not yet commenced.

¹⁷ Section 8(1) of the Act.

¹⁸ Section 13(1)(d) of the Act.

¹⁹ Section 12(6) of the Act.

²⁰ Section 15(1).

D. Choice on Termination of Pregnancy Act, No. 92 of 1996²¹

1. A “**minor**” for purposes of this Act means any female person under the age of 18 years.
2. The Act provides that in the case of a pregnant minor, a medical practitioner, registered midwife or registered nurse is obliged to advise such **minor to consult, *inter alia*, her parents or guardian** before such pregnancy is terminated, provided that the termination of a pregnancy **may not be denied** because a minor chooses not to consult them.²²
3. The Act further provides that the **identity** of a woman (which definition includes any female person of any age - and therefore a female minor) who has requested / obtained a termination of pregnancy, **shall remain confidential at all times** unless she herself chooses to disclose such information.²³
4. A member of the Executive Council who is responsible for health in that province may, in consultation with the Minister of Health, make **regulations** necessary for the proper implementation of the Act.²⁴ These regulations include a provision that a woman requesting the termination of her pregnancy must be informed that the process of **counselling is private and confidential**, unless she chooses to disclose such information.²⁵

²¹ The 2004 amendment to this Act has been declared unconstitutional on 17 August 2006 as a result of the parliamentary process followed and not the content or substance thereof

²² Section 5(3)

²³ Section 7(5)

²⁴ Section 9

²⁵ Regulation 7(c) of Government Notice R168, in Government Gazette 17746 of 31 January 1997

E. **Electronic Communications and Transactions Act, No 25 of 2002 ("ECT Act")**

1. It is to be noted that the ECT Act only deals with **electronic information**.
2. The ECT Act defines **personal information** as *inter alia* information about an **identifiable** individual, including but not limited to information relating to the physical or mental health or well-being or blood type of the individual. This definition corresponds with the definition of personal information as provided for in PAIA and the Protection of Personal Information Bill.
3. A **data subject** is defined as any natural person from or in respect of whom personal information has been electronically requested, collected, collated, processed or stored.
4. **Data** for purposes of this Act means electronic representations of information in any form whereas a **data controller** means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.
5. The "data controller" in the ECT Act and the "responsible party" in the Protection of Personal Information Bill is the same person. The only difference is that the "data controller" only processes **electronic information** whereas the "responsible party" processes **both electronic and manual information**.
6. For purposes of this report, health care providers, medical schemes, medical scheme administrators, managed care organisations, and data management companies are considered to be data controllers and as such, are subject to the provisions of the ECT Act.
7. The ECT Act applies in respect of any **electronic transaction or data message** subject to certain exclusions. The ECT Act must also not be interpreted as to exclude any statutory law or common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in the ECT Act.
8. Chapter 8 of the ECT Act applies to personal information that has been obtained through **electronic transactions**. It should be remembered that a **data controller** in the ECT Act **may voluntarily subscribe** to the principles outlined in Chapter 8 of the Act by recording such fact in any agreement with a data subject. **Chapter 8 is therefore not compulsory**. The reason why these provisions are not mandatory is because this Chapter will fall away once the Protection of Personal Information Bill is in place. These provisions are regarded as an **interim arrangement**.

9. Subject to what is stated in paragraph 8 above, it is to be noted that:
- 9.1. a data controller must have the **express written permission** of the data subject for the processing, collection, collation, or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law²⁶;
 - 9.2. the data controller must **disclose in writing** to the data subject the **specific purpose** for which any personal information is being requested, collected, collated, processed or stored.²⁷ This once again emphasises the need for understanding the intended use of PHI;
 - 9.3. a data controller **shall not disclose** any of the personal information held by it to a **third party**, unless required or permitted by law or specifically authorised to do so in writing by the data subject²⁸;
 - 9.4. a party controlling personal information may use that personal information to compile profiles for **statistical purposes** and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party i.e. the data is **unidentifiable or anonymised**.²⁹ The size of the sample of the unidentifiable or anonymised data must also be large enough to avoid identification by deduction if the sample is too small.
10. The Minister of Communications ("the Minister") may also, by notice in the *Gazette*, **declare** certain **classes of information** which is of importance to the protection of the national security of the RSA or the economic and social well-being of its citizens to be "**critical data**", **establish procedures** to be followed in the identification of critical databases³⁰ and **determine the requirements and procedures** for the registration of critical databases.³¹
11. A "**critical database**" means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted. **It is to be noted however, that to date no critical databases have been identified by the Minister of Communications.** A new Protection of Information Bill (to replace the previous 1984 Act) is being drafted by the National Intelligence Ministry and may make this section of the ECT Act redundant.
12. "**Registration of a critical database**" means **recording the following information in a register** maintained by the Department of Communications ("the Department") (or by such other body as the Minister may specify) –
- 12.1. the name, address and contact details of the person responsible for the management and control of a critical database ("**the critical database administrator**");

²⁶ Section 51(1)

²⁷ Section 51(3)

²⁸ Section 51(6)

²⁹ Section 51(9)

³⁰ Section 53

³¹ Section 54(1)

- 12.2. the **location** of the critical database, including the locations of component parts; and
 - 12.3. a general **description of the categories or types of information** stored in the critical database **excluding the contents of such critical database**.³²
13. The **Minister may prescribe minimum standards** or prohibitions in respect of, *inter alia*, the general management of critical databases, access to, transfer and control of critical databases, and any matter required for the adequate protection, management and control of critical databases.³³
 14. **Information contained in the register** referred to in **paragraph 12** above **must not be disclosed** to any person other than to employees of the Department who are responsible for the keeping of the register, provided that this provision does not apply in respect of information which is disclosed³⁴ -
 - 14.1. to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;
 - 14.2. to government agencies responsible for safety and security in the RSA pursuant to an official request;
 - 14.3. to a cyber inspector for purposes of an audit (as discussed in **paragraph 15** below);
 - 14.4. pursuant to sections 11 and 30 of the Promotion of Access to Information Act, 2000; or
 - 14.5. for the purposes of any civil proceedings which relate to the critical data or parts thereof.
 15. The **Director-General** of the Department **may cause audits to be performed to evaluate compliance** by the critical database administrator. The audit may be performed by either cyber inspectors (i.e. employees of the Department) or an independent auditor.³⁵ Should the audit reveal non-compliance by the critical database administrator, the Director-General must notify the critical database administrator thereof in writing, stating, *inter alia*, the period within which the remedial action must be performed. A critical database administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence.³⁶

³² Section 54(2)

³³ Section 55(1)

³⁴ Section 56

³⁵ Section 57.

³⁶ Section 58.

F. **Health Act, No. 63 of 1977**

1. This Act provides that when a medical practitioner, a practitioner registered as such in terms of the Associated Health Service Professions Act, 1982 (Act 63 of 1982), or any other person legally competent to diagnose and treat a person with regard to notifiable medical conditions, for gain, **diagnoses a notifiable medical condition** in a person he shall report his findings to the appropriate authority as stipulated in regulation 19.³⁷
2. The Minister of Health, after consultation with the Minister of Manpower Utilisation and the Minister of Mineral and Energy Affairs, declares medical conditions to be a notifiable medical condition in terms of section 45 of this Act.
3. On making the report as provided for in **paragraph 1**, the following information must be furnished in respect of the patient:
 - 3.1. Name;
 - 3.2. Age;
 - 3.3. Sex;
 - 3.4. Population group;
 - 3.5. Identity number or if the identity number is not available, the date of birth;
 - 3.6. the address, place of work or school of the person in respect of whom the report is made;
 - 3.7. The date of commencement of the notifiable medical condition; and
 - 3.8. Any available information concerning the probable place and source of infection.

³⁷ Regulations Relating to Communicable Diseases and the Notification of Notifiable Medical Conditions, published under Notice R2438 in *Government Gazette* 11014 of 30 October 1987.

G. Health Professions' Act, No. 56 of 1974 & Regulations ("HPA") and Ethical Rules of the HPCSA

1. Professions falling under the following Professional Boards are covered by the HPA and Ethical Rules of the HPCSA:
 - 1.1. Dental therapy and oral hygiene;
 - 1.2. Dietetics;
 - 1.3. Emergency care;
 - 1.4. Environmental health;
 - 1.5. Medical and dental;
 - 1.6. Medical technology;
 - 1.7. Occupational therapy, medical orthotics/prosthetics and art therapy;
 - 1.8. Optometry and dispensing opticians;
 - 1.9. Physiotherapy, podiatry and biokinetics;
 - 1.10. Psychology;
 - 1.11. Radiography and clinical technology; and
 - 1.12. Speech, language and hearing professions.

2. **Guidelines for Good Practice in Medicine, Dentistry and the Medical Sciences - Confidentiality: Protecting and Providing Information (Booklet 14)**
 - 2.1. These guidelines define **anonymised data** as data from which the patient cannot be identified by the recipient of the information.
 - 2.2. **Consent** for purposes of these guidelines means an agreement to an action based on knowledge of what the action involves and its likely consequences.
 - 2.3. **Health care team** is defined as the team who comprise of the people providing clinical services for each patient and the administrative staff who directly support those services.
 - 2.4. Guideline 3.1 pertaining to the **disclosure of information** as well as the sharing of information with others providing care, states as follows: "*Where patients have consented to treatment, express consent is not usually needed before relevant personal information is shared to enable the treatment to be provided. For example, express consent would not be needed before general practitioners disclose relevant personal information so that a medical secretary can type a referral letter. Similarly, where a patient has agreed to be referred for an X-ray, referring practitioners may make relevant information available to diagnostic radiologists when requesting an X-ray. Practitioners cannot treat patients safely, nor provide the continuity of care, without having relevant information about the patient's condition and medical history*".

- 2.5. Health care providers should make sure that patients are aware that personal information about them will be **shared** within the health services team, unless they object. The patient must be aware of the reasons for which disclosure of PHI are required. A health care provider must respect the wishes of any patient who objects to particular information being shared with other providing care, except where this would put others at **risk of death** or **serious harm**.
- 2.6. These guidelines provide that anyone receiving personal information in order to provide care is bound by a **legal duty of confidence**, whether or not they have contractual or professional obligations to protect confidentiality.
- 2.7. The **automatic transfer** of personal information to a **registry**, whether by electronic or other means, before informing the patient that information will be passed on, is unacceptable, save in the most exceptional circumstances. These would be where a court has already decided that there is such an overwhelming public interest in the disclosure of information to a registry that patients' rights to confidentiality are overridden; or where the health care provider is willing and able to justify the disclosure, potentially before a court or to the Board, on the same grounds.³⁸
- 2.8. Guideline 5.4.1 provides that where the patient is incapable of giving consent to disclosure because of **immaturity, illness or mental incapacity**, the health care provider should try to persuade patient to allow an appropriate person to be involved in the consultation. If the patient refuses and the health care provider is convinced that it is essential, in his/her medical interests, the health care provider may disclose relevant information to an appropriate person or authority. Once the Children's Act is promulgated, this guideline may have to be reviewed.
- 2.9. Guideline 7 sets out the appropriate steps to be followed for the **electronic processing of information**. The health care provider must *inter alia* be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by electronic means. Furthermore, a health care provider may constitute a data controller as provided for in the ECT Act and may therefore be bound by the provisions stipulated under **Section E of Chapter IX**.

3. **Guidelines for Good Practice in Medicine, Dentistry and the Medical Sciences: Guidelines on Keeping Patient Records (Booklet 11)**

Guideline 8.3 provides that information about the **termination of pregnancy** may not be divulged to any party, except the patient herself, regardless of the age of the patient. **Health care providers will have to be cautious when an account is rendered for the termination of a pregnancy where the medical scheme member is not the person that has terminated the pregnancy i.e. a dependant has undergone the termination of pregnancy.**

³⁸ Guideline 5.1.1(f)

4. **Ethical Rules of Conduct for Practitioners Registered under the HPA – Government Gazette Number 29079, 4 August 2006**

- 4.1. Rule 13(1) caters for professional confidentiality and states that a practitioner may divulge information only:
 - 4.1.1. in terms of a statutory provision;
 - 4.1.2. at instruction of a court of law; or
 - 4.1.3. where justified in the public interest.
- 4.2. Rule 13(2) provides that any other information may only be divulged by a practitioner:
 - 4.2.1. with express consent of the patient;
 - 4.2.2. in the case of a minor < 14 with written consent of his/her parent / guardian;
 - 4.2.3. in the case of a deceased patient with written consent of his/her next-of-kin / executor.
- 4.3. A psychologist may disclose confidential information only with written informed consent of the client concerned³⁹;
- 4.4. A psychologist engaging in electronically transmitted services must ensure that confidentiality and privacy are maintained and must inform a client of the measures taken to maintain confidentiality.

5. **General**

- 5.1. The HPCSA must ensure that each practice retains confidentiality in accordance with relevant legislation. Health care providers are responsible for confidentiality within their practices and must therefore ensure that they have confidentiality agreements in place with:
 - 5.1.1. their employees;
 - 5.1.2. practice management application software vendors;
 - 5.1.3. accounting bureaus;
 - 5.1.4. other contracted third parties who may have access to identifiable patient information in their records and/or systems.
- 5.2. The provisions of the above Ethical Rules may have to be revised once the **Children's Act** has been promulgated insofar as these rules relate to consent relating to a minor.

³⁹ Rule 24 of Annexure 12 to Schedule

- H. **Medical Schemes Act No. 131 of 1998 and Regulations thereto, as amended ("the MSA")**
1. Section 57 provides that the **Board of Trustees** of a medical scheme shall take all reasonable steps to protect the confidentiality of medical records concerning any member's state of health.
 2. Section 59 requires a supplier of service who has rendered any service to a medical scheme beneficiary in terms of which an account has been rendered to, **notwithstanding the provisions of any other law**, furnish to the member concerned an account or statement reflecting such particulars as may be prescribed. Regulation 5(f) states that the account or statement **must** contain **the relevant diagnostic and such other item code numbers that relate to such relevant health service**.
 3. Regulation 15D requires a medical scheme to ensure that where **managed health care** is undertaken either by the medical scheme itself or by a managed health care organisation that a written protocol is in place that contains provisions for ensuring confidentiality of clinical and proprietary information.
 4. Regulation 15J emphasises that notwithstanding anything to the contrary to the regulations to the MSA, any information pertaining to the **diagnosis, treatment or health** of any medical scheme beneficiary must be treated as confidential.
 5. From a strictly legal perspective, medical schemes are not in a position to use the ICD-10 information for any other reason than that stipulated in section 59 of the MSA and elaborated on in regulation 5. The CMS may have to consider changes to the MSA depending on the intended use of ICD-10 codes. This is critical as a patient should be guaranteed that their ICD-10 codes will only be used for those reasons for which they gave informed consent.
 6. The **accreditation standards** of the CMS for **medical schemes, medical scheme administrators and managed care organisations** require the maintaining of confidentiality, security and integrity of data and information.
 7. The document published by the CMS on the Findings and Recommendations of the Governance Theme Project titled "Putting Members First: Towards Better Governance of Medical Schemes" dated May 2006 emphasised the need for **medical schemes to contract with all their third party service providers** (including but not limited to administrators, managed care companies, switching companies and data management / data transfer companies) to ensure the **scrupulous protection of the confidentiality of individual member information**. In particular, these third party service providers must undertake to the medical scheme in question not to use identifiable patient information for purposes other than those stipulated in the MSA or other relevant legislation.

8. The CMS have formulated a **uniform guideline** for the industry that sets out specifically the purpose for disclosure of information in terms of ICD-10 diagnosis, the intended recipients of such information and what the information will be used for. This document was published on the website of the CMS on 9 February 2007 under the heading "Notice to Consumers: ICD-10 Coding: All you need to know as a consumer".
9. The CMS has over the past few years put several processes in place that addresses many of the concerns around PHI and informed consent for the transfer of PHI to relevant parties. In addition to these, several new initiatives are being embarked upon, that will further address these issues.
10. Existing and new initiatives of the CMS include:
 - 10.1. Accreditation of Managed Care entities;
 - 10.2. Accreditation of Administrators;
 - 10.3. Accreditation of Brokers;
 - 10.4. Registration of medical schemes and their rules;
 - 10.5. Development of requirements for medical scheme application forms;
 - 10.6. Development of guidelines for marketing materials; and
 - 10.7. Development of communiqués to consumers and health service providers.

1. **Mental Health Care Act, No. 17 of 2002**

1. The **person, human dignity and privacy** of every mental health care user must be respected.⁴⁰
2. A person or health establishment **may not disclose** any information which a mental health care user is entitled to keep **confidential in terms of any other law**.⁴¹
3. A health care provider or a health establishment **may provide care, treatment and rehabilitation services to or admit a mental health care user only if –**
 - 3.1. the user has **consented** to the care, treatment and rehabilitation services or to admission;
 - 3.2. authorised by a **court order** or a **Review Board**; or
 - 3.3. due to mental illness, any **delay** in providing care, treatment and rehabilitation services or admission may result in the –
 - 3.3.1. **death** or irreversible harm to the health of the user;
 - 3.3.2. user inflicting **serious harm** to himself or herself or others; or
 - 3.3.3. user causing serious **damage to or loss of property** belonging to him or her or others⁴².
4. Any person or health establishment that provides care, treatment and rehabilitation services to a mental health care user or admits the user because due to such person's mental illness, any delay in providing care, treatment and rehabilitation services or admission may result in the circumstances discussed above, must **report this fact in writing** to the relevant **Review Board** and may not continue to provide care, treatment and rehabilitation services to the user concerned for longer than 24-hours unless an application in terms of Chapter V of the Act is made within the 24-hour period⁴³.
5. Subject to the above, a mental health care user **may not be provided with assisted care, treatment and rehabilitation services at a health establishment as an outpatient or inpatient without his or her consent, unless** a written application for care, treatment and rehabilitation services is made to the **head of the health establishment** concerned and he or she approves it; and at the time of making the application -
 - 5.1. there is a reasonable belief that the mental health care user is suffering from a mental illness or severe or profound mental disability, and requires care, treatment and rehabilitation services for his or her **health or safety, or for the health and safety of other people**; and
 - 5.2. the mental health care user is **incapable of making an informed decision** on the need for the care, treatment and rehabilitation services⁴⁴.
6. A mental health care user must be provided with care, treatment and rehabilitation services **without his or her consent** at a health establishment on an outpatient or inpatient basis if -

⁴⁰ Section 8(1) of the Act.

⁴¹ Section 13(1) of the Act.

⁴² Section 9(1)

⁴³ Section 9(2) and Regulation 8

⁴⁴ Section 26

- 6.1. an **application in writing** is made to the head of the health establishment concerned to obtain the necessary care, treatment and rehabilitation services and the application is granted;
- 6.2. at the time of making the application, there is **reasonable belief** that the mental health care user has a mental illness of such a nature that -
 - 6.2.1. the user is likely to **inflict serious harm** to himself or herself or others; or
 - 6.2.2. care, treatment and rehabilitation of the user is necessary for the **protection of the financial interests or reputation** of the user; and
- 6.3. at the time of the application the mental health care user is **incapable of making an informed decision** on the need for the care, treatment and rehabilitation services and is unwilling to receive the care, treatment and rehabilitation required⁴⁵.
7. **No psychosurgery** may be performed on a mental health care user who is **not capable of giving informed consent** for such surgery⁴⁶.
8. Regulation 35(1) provides that an **involuntary mental health care user, an assisted mental health care user, a state patient or a mentally ill prisoner** who is capable of giving informed consent to treatment or an operation, must decide whether to have treatment or an operation or not.
9. In terms of Regulation 35(2), **where a mental health care provider deems a user to be incapable of consenting** to treatment or an operation due to mental illness or intellectual disability, then a **curator**, if a court has appointed one, a **spouse, next of kin, a parent or guardian, a child over the age of 18, a brother or sister, or a partner or associate, may consent** to the treatment or operation.
10. Regulation 35(3) provides that the **head of the health establishment** where the mental health care user resides or the head of a facility where the mental health care user resides, **may grant consent** to treatment or an operation if -
 - 10.1. none of the persons referred to in **paragraph 9** above is available and unsuccessful attempts have been made to locate them and this has been confirmed in writing;
 - 10.2. the relevant alternatives have been discussed with the head of the health establishment or the head of the licensed facility concerned above and that head is satisfied that the most appropriate intervention is to be performed; and
 - 10.3. the medical practitioner who is going to perform that operation recommends the treatment or operation.
11. In terms of Regulation 33, the provisions of regulation 35 (discussed above) relating to consent must be adhered to in the case of **electro-convulsive treatment**.

⁴⁵ Section 32

⁴⁶ Regulation 32

J. **National Health Act, No. 61 of 2003 (“the NHA”)**

1. The NHA provides that subject to the National Archives of South Africa Act, No. 43 of 1996 , and PAIA⁴⁷, the person in charge of a health establishment (public and private) must ensure that a **health record** containing such information as may be prescribed is created and maintained at that health establishment for every user of health services.⁴⁸
2. A **user** is defined in terms of the NHA as *inter alia* a person receiving treatment in a health establishment.
3. All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is **confidential**.⁴⁹
4. Disclosure of confidential information may take place as provided for in section 14(2) of the NHA (for example, the **user consents to that disclosure in writing**).
5. A health worker or any health care provider that has access to the health records of a user **may disclose** such personal information to any other person, health care provider or health establishment as is **necessary for any legitimate purpose** within the ordinary scope of his or her duties where such access or disclosure is in the interests of the user.⁵⁰ For purposes of this paragraph personal information bears the same meaning as per the definition in PAIA.⁵¹
6. The person in charge of a health establishment in possession of user’s health records must set up **control measures** to prevent unauthorised access to those records and to the storage facility in which, or system by which records are kept.⁵² Should a person fail to perform this duty, such a person commits an offence and is liable, on conviction, to a fine or to imprisonment.
7. Every health care provider must inform a user of the benefits, risks, costs and consequences generally associated with each diagnostic procedure and treatment option available to the user.⁵³ A user must be informed in a language that he/she understands and in a manner which takes into account the user’s level of literacy.⁵⁴
8. Subject to a user’s participation in decisions, health services may not be provided to a user without the user’s informed consent, unless:⁵⁵
 - 8.1. the user is unable to give informed consent and such consent is given by a person:

⁴⁷ Promotion of Access to Information Act, No. 2 of 2000

⁴⁸ Section 13

⁴⁹ Section 14(1)

⁵⁰ Section 15(1)

⁵¹ See **paragraph 2 of Section M** above

⁵² Section 17(1)

⁵³ Section 6(1)

⁵⁴ Section 6(2)

⁵⁵ Section 7(1)

- 8.1.1. **mandated** by the user **in writing** to grant consent on his or her behalf; or
- 8.1.2. **authorised** to give such consent in terms of **any law or court order**;
- 8.2. the user is unable to give informed consent and no person is mandated or authorised to give such consent, and the consent is given by the spouse or partner of the user or, in the absence of such spouse or partner, a parent, grandparent, an adult child or a brother or a sister of the user, in the specific order as listed;
- 8.3. the provision of a health service without informed consent is authorised in terms of any law or a court order;
- 8.4. failure to treat the user, or group of people which includes the user, will result in a serious risk to public health; or
- 8.5. any delay in the provision of the health service to the user might result in his or her death or irreversible damage to his or her health and the user has not expressly, impliedly or by conduct refused that service.
9. A health care provider must take all reasonable steps to obtain the user's informed consent for the purposes of the provision of a health service.⁵⁶
10. "Informed consent" relating to the provision of a health service means consent for the provision of a specified health service given by a person with legal capacity to do so and who has been informed.⁵⁷
11. If a user is unable to participate in a decision affecting his or her personal health and treatment, he or she must be informed after the provision of the health service in question unless the disclosure of such information would be in contrary to the user's best interest.⁵⁸
12. Section 9 of the NHA caters for the provision of a health service without consent and provides that the health establishment must notify the head of provincial department in the province in which that health establishment is situated.
13. Section 74 of the NHA provides for the establishment of a comprehensive **national health information system**. The Minister of Health may prescribe **categories or kinds of data for submission and collection** and the **manner and format** in which, and by whom, the data must be compiled or collated and submitted to the National Department. The details of such a system and its requirements are still to be established, but it would seem as if there would be certain minimum requirements with regards to information technology. These minimum requirements will have to be taken into account by medical schemes or their administrators for the disclosure of PHI going forward. This system will however be critical for the notion of a **patient centred information system**.

⁵⁶ Section 7(2)

⁵⁷ Section 7(3)

⁵⁸ Section 8(3)

14. **No regulations** relating to the National Health Information System as provided for in the NHA have to date been published.

- K. **Nursing Act, No. 50 of 1978 (“the Current Nursing Act”), Nursing Act, No. 33 of 2005 (“the New Nursing Act”) and Rules issued by the South African Nursing Council (“SANC”)**
1. The Minister of Health shall be entitled, on the recommendation of the SANC, by notice in the *Gazette* to **specify the acts or omissions** in respect of which the SANC may take **disciplinary steps** under Chapter 4 of the Current Nursing Act, provided that the powers of the SANC to inquire into and deal with any complaint, charge or allegation, shall not be limited to the acts or omissions so specified.⁵⁹
 2. Section 38A of the Current Nursing Act or section 56 of the New Nursing Act sets out circumstances under which registered nurses are authorised, *inter alia*, to diagnose illness and/or prescribe medicines.
 3. The disclosure by a nurse of **any information concerning a patient** obtained in the course of the professional activities of the nurse, shall constitute an act in respect of which the SANC may take disciplinary steps - provided that this rule shall not be applicable if such information is made known with the explicit consent of the patient or, in the case of a minor, with the consent of the parent or guardian, or where instructed thereto by a court of law or where a nurse is otherwise lawfully bound thereto, or where such disclosure is in the interest of the patient, or where such disclosure is made in a professional consultation with anybody involved in the treatment of the patient or, in the exclusive interest of the patient, with somebody else.⁶⁰ The SANC rules may have to be reviewed once the Children's Act has been promulgated insofar as these rules relate to consent of the parent or guardian as opposed to consent by the minor.
 4. The commencement date of the **New Nursing Act must still be proclaimed**. In terms of the New Nursing Act, it is the duty of SANC to ensure that **persons registered** in terms of the New Nursing Act behave towards **users of health services** in a manner which **respects their constitutional rights to human dignity**, bodily and psychological integrity and equality.⁶¹ The constitutional right to human dignity will encompass the right to privacy. Further, the Minister of Health is granted similar rights, after consultation with SANC, to make regulations relating to circumstances in which a name may be removed from the register⁶² and generally any matter which the Minister considers necessary to achieve the objects of the New Nursing Act.⁶³

⁵⁹ Section 35 of the Current Nursing Act

⁶⁰ Rule 15 of the SANC Rules setting out the Acts or Omissions in respect of which the Council may take disciplinary steps (Government Notice R.387 dated 15 February 1985, as amended by R. 866 dated 24 April 1987 and R. 2490 dated 26 October 1990).

⁶¹ Section 4(1)(f) of the New Nursing Act

⁶² Section 58(1)(k) of the New Nursing Act

⁶³ Section 58(1)(s) of the New Nursing Act

5. After the commencement of the New Nursing Act, the **transitional provisions** contained in section 61 of such Act shall apply. These transitional provisions include that any notice, **regulation** etc **made in terms of any law repealed** by the New Nursing Act (e.g. the Rules made by the Minister in terms of the Current Nursing Act) **shall, unless inconsistent** with the New Nursing Act, be deemed to have been made under the corresponding provision of the New Nursing Act.⁶⁴

⁶⁴ Section 61(1) of the New Nursing Act

L. **Pharmacy Act, No. 53 of 1974 & Regulations and Ethical Rules issued by the South African Pharmacy Council (“SAPC”)**

1. A pharmacy shall, subject to such conditions as may be prescribed, be conducted under the continuous personal supervision of a pharmacist, in accordance with **good pharmacy practice** as determined in the rules made by the council.⁶⁵
2. The SAPC shall be entitled to make rules as to a **code of conduct** for pharmacists and what constitutes good pharmacy practice.
3. The **disclosure of confidential information** obtained in the course of the professional activities of a pharmacist – except with the **express consent** of the patient or, in the case of a minor, with the consent of the parent or guardian, or where such information must be furnished to a person authorised by law to request it – unless such disclosure is in the interest of the patient, shall be deemed to be unethical or unprofessional conduct subject to disciplinary steps by the SAPC.⁶⁶
4. The guideline as per paragraph 3 above may be in conflict with the provisions of the **Children’s Act**, once promulgated, insofar as it relates to consent of the parent or guardian as opposed to consent by the minor and may therefore have to be reviewed.
5. Regulation 28(5) of the Medicines and Related Substances Act 101 of 1965 states that the prescriber must keep records of the diagnosis relevant to the prescription and **where the patient consents, indicate the diagnosis on the prescription.**
6. The SAPC holds the view that the decision to disclose or withhold PHI (including diagnosis) rests with the patient and the role of the prescriber is to properly educate patients on the importance and consequence of disclosure of their PHI (including diagnosis) to other health care providers.

⁶⁵ Section 22(4).

⁶⁶ Rule 9 of the Rules Relating to Acts or Omissions in respect of which the Council may take Disciplinary Steps

M. **Promotion of Access to Information Act, No. 2 of 2000 (“PAIA”)**

1. The operation of the right of access to information is the subject of PAIA.
2. **Personal information** is defined in PAIA as, *inter alia*, information about an identifiable individual, including but not limited to information relating to the physical or mental health or well-being or blood type of the individual. This definition corresponds with the definition of personal information as provided for in the ECT Act and the Protection of Personal Information Bill.
3. Section 63(1) provides that the head of a private body must refuse a request for access to a record of the body if its disclosure would involve the **unreasonable disclosure of personal information** about a third party, including a deceased individual. Section 34 contains a similar provision insofar as public bodies are concerned.
4. Section 63(2)(a) however allows for disclosure where the individual has **consented in writing** where the record is held by a private body. Section 34(2)(a) contains a similar provision where the record is held by a public body.
5. A record held by either a private body or a public body may however not be refused insofar as it consists of information about the physical or mental health or well being of an individual who is under the care of the requestor and who is:
 - 5.1. under the age of 18 years; or
 - 5.2. incapable of understanding the nature of the request, and if giving access would be in the individual's best interests⁶⁷.
6. It is to be noted that the contents of **paragraph 5.1** conflicts with the provisions of Section 13(1)(d) of the **Children's Act**, No. 38 of 2005.
7. Mandatory disclosure in the **public interest** is required if the disclosure of the record would reveal evidence of **imminent and serious public safety or environmental risk** and the **public interest** in the disclosure of the record clearly **outweighs** the **harm contemplated**.⁶⁸

⁶⁷ See Sections 34(2)(d) and 63(2)(d) of PAIA in this regard.

⁶⁸ See Sections 46 and 70 of PAIA in this regard.

N. **Protection of Personal Information Bill**

1. **General privacy principles:**

1.1. Information privacy is not regarded as a domestic policy problem. The information privacy principles set out in the Protection of Personal Information Bill are regarded worldwide as the internationally accepted standard for the protection of personal information. They emanate from two international instruments:

1.1.1. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and

1.1.2. the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

1.2. The abovementioned instruments should furthermore be read with the European Union Data Protection Directive of 1994 which provides for the harmonisation of member states' laws. Important for countries outside Europe is that Articles 25 and 26 of the Directive stipulate that personal data should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection". If a country can not do that, information from the EU countries may not be shared with such a country.

1.3. These principles, known as the "Principles of Data Protection", therefore form the basis worldwide of both legislative regulation and self-regulating control. Compliance with these principles is also regarded as good business practice.

2. The draft Protection of Personal Information Bill ("the Bill") does not apply to the processing of personal information that has been **de-identified to the extent that it cannot be re-identified again**.

3. This Bill will also not affect the operation of any enactment that makes provision with respect to the processing of personal information and is capable of operating **concurrently** with this Bill.

4. This Bill when promulgated will **bind the State** and hence the Department of Health.

5. In terms of the Bill the act of "**processing**" personal information, **includes**, *inter alia*, "**any operation...concerning personal information, including...dissemination by means of transmission, distribution...**".⁶⁹

⁶⁹ Section 2

6. **Personal information** is defined as *inter alia* information about an identifiable, natural person including, but not limited to physical or mental health, well-being or disability. This definition in essence corresponds with the definitions of personal information as provided for in PAIA and the ECT Act.
7. The act of processing personal information of a "data subject" is conducted by a "processor" on behalf of a "responsible party" or by a "responsible party" itself.
8. A "**data subject**" is defined as the person to whom personal information relates. In the health care industry this would constitute the **patient**.
9. The "**processor**" is defined as the person or body which processes personal information for the responsible party, without coming under the direct authority of that party i.e. the "processor" is an **additional responsible party** where the original responsible party does not process the information it/him/herself, but, for instance, contracts out the processing to a third party that is not under the direct authority of the original responsible party. Special rules apply in this circumstance.
10. In the health care industry processors could constitute **health care providers, medical schemes, medical scheme administrators, managed care organisations, data management companies and any other entity switching or processing PHI**.
11. The "**responsible party**" is defined as the natural person, juristic person, administrative body or any other entity which, alone or in conjunction with others, **determines the purpose of and means for processing personal information**⁷⁰. Any of the following parties may constitute a "responsible party" for purposes of this report if such a party is the recipient of PHI (for example an ICD-10 code linked to an identifiable patient):
 - 11.1. health care provider;
 - 11.2. a medical scheme;
 - 11.3. the CMS;
 - 11.4. the REF (once implemented); and/or
 - 11.5. the Department of Health / State.
12. "**Processing**" is defined as any operation or any set of operations concerning personal information, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information.
13. **Personal information must be processed lawfully**. It is, however, not the intention of this Bill to obstruct the lawful flow of information. In fact, one of the objects of this Bill is to harmonise the rules of processing in order to **encourage the flow of information**.
14. The Bill contains various instances in which personal information may be processed, the most important of which being when the "**data subject/the medical scheme beneficiary has given consent**" for the processing".⁷¹

⁷⁰ Please also refer to paragraph 5 of Section E of Chapter IX.

⁷¹ Section 9(1)(a)

15. The data subject must as far as reasonably practicable, **be aware of the purpose for which the information is being collected and the intended recipients** of the information.⁷²
16. Principle 3 of the Bill contains **limitations on further processing** of personal information, and provides that personal information **may not be further processed in any way incompatible with a purpose** for which it has been collected.⁷³
17. The Bill contains various points for consideration by the responsible party in assessing whether processing is incompatible as referred to above, including “the relationship between the purpose of the intended further processing and the purpose for which the information has been obtained...”.⁷⁴
18. **Further processing** of personal information will however **not be** regarded as **incompatible** where the **data subject authorises** such further processing.⁷⁵
19. Principle 6 of the Bill contains various security safeguards for the protection of personal information and requires that a **written agreement** be concluded between a responsible party and a processor, which agreement must include **an obligation to establish and maintain security safeguards**.⁷⁶ This principle will also support the conclusion of written agreements by medical schemes as provided for in **paragraph 7, Section H of Chapter IX**.
20. The responsible party must further **satisfy itself that the processor:**
 - 20.1. establishes and maintains the **information security safeguards** specified in section 17(2) of the Bill; and
 - 20.2. **complies with the obligations of the responsible party relating to security measures**, contained in section 17 of the Bill.⁷⁷
21. The Bill places an **overriding obligation on the responsible party** to ensure that, inter alia, the **measures** that give effect to the Principles discussed above, **are complied with**.⁷⁸
22. The proposed Bill also prohibits the processing of personal information concerning a person's **health or sexual life** except where the data subject has given his / her **explicit consent** to the processing of information.⁷⁹

⁷² Section 12(1)

⁷³ Section 14(1)

⁷⁴ Section 14(2)

⁷⁵ Section 14(3)(1)(a)

⁷⁶ Section 19(2)

⁷⁷ Section 19(3)

⁷⁸ Section 23

⁷⁹ Section 24

23. This prohibition does not apply where the processing is carried out by medical professionals, health care institutions or facilities or social services, provided that this is **necessary for the proper treatment and care of the data subject**, or for the **administration of the institution or professional practice concerned**.⁸⁰ In these two instances, the information may only be processed by persons subject to an **obligation of confidentiality** by virtue of office, employment, profession or legal provision, or under a written agreement.⁸¹
24. Where responsible parties personally process information and are not already subject to an obligation of confidentiality by virtue of office, profession or legal provision, **they are required to treat the information as confidential**, except where they are required by law or in connection with their duties to communicate such information to other parties who are authorised to process such information in accordance with [paragraph 23](#) above.
25. Personal information concerning **inherited characteristics** may only be processed, where this processing takes place with respect to the data subject from whom the information concerned have been obtained, unless:
- 25.1. a serious medical interest prevails, or
 - 25.2. the processing is necessary for the purpose of scientific research or statistics.
26. The responsible party must take the **reasonably practicable steps**, given the purpose for which personal information is collected or subsequently processed, to ensure that the personal information is **complete, not misleading, up to date and accurate**.
27. Section 33 of the Bill provides that the Information Protection Commission may **exempt** a responsible party from the information protection principles if it is satisfied that in the special circumstances of the case :
- 27.1. the **public interest** in that processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from that processing; or
 - 27.2. that processing involves a **clear benefit** to the data subject or a third party that outweighs any interference with the privacy of the data subject or third party that could result from that processing.
28. It is important to note that this Bill requires a responsible party to implement **appropriate technical and organizational measures** to secure:
- 28.1. The integrity of personal information by safeguarding against the risk of loss of, or damage to, or destruction of personal information; and
 - 28.2. Against the unauthorised or the unlawful access to or processing of personal information.

⁸⁰ Section 29(1)(a)

⁸¹ Section 29(2)

29. This Bill, once promulgated, will necessitate the **conclusion of confidentiality agreements** between medical schemes and their service providers (administrators, managed care companies, switching companies and data management / data transfer companies) to ensure compliance with the provisions of the Bill. This also supports the view of the CMS as set out in **paragraph 7, Section H of Chapter IX**.

- O. **Sterilisation Act, No. 44 of 1998 and regulations published under Government Notice R872 on 16 July 1999**
1. A person may be sterilized if he/she is **capable of consenting and at least 18** years old.⁸²
 2. Sterilization of persons younger than 18 years, may only be performed if failure to do so will **jeopardize the person's life or seriously impair his/her health**.⁸³ A person under the age of 18 years may however be sterilized if consent is given by a person lawfully entitled to give consent (i.e. a **parent, guardian, curator** etc.) and an independent medical practitioner, who before a panel is convened as set out in the Act, has consulted the person to be sterilized and has provided a written opinion that the sterilization is in the best interest of the person.⁸⁴ The provisions of this section of the Act may be in conflict with the Children's Act insofar as it relates to consent of the parent or guardian as opposed to consent by the minor.
 3. A person who is **incapable of, or incompetent to consent** may be sterilized in terms of the Act, **upon a request** from, *inter alia*, the parent, spouse, guardian or curator of such person, and if a panel contemplated in the Act after considering all the relevant information concurs that the sterilization may be performed, and if the person is, *inter alia*, mentally disabled to such an extent that he/she is incapable of making a decision about contraception or sterilization.⁸⁵
 4. The person in charge of a facility⁸⁶ must be notified of every sterilization performed in that facility and must **keep a record** of every such sterilization.⁸⁷
 5. Neither the Act nor the Regulations, makes any reference to any obligations of confidentiality in respect of the sterilization procedure.

⁸² Section 2(1).

⁸³ Section 3(a).

⁸⁴ Section 3(c).

⁸⁵ Section 3(1).

⁸⁶ A "facility" is designated as a place where sterilization may take place in writing by a member of the Executive Council responsible for health in a province, as set out in Section 5.

⁸⁷ Section 6.

P. **Traditional Health Practitioners Act 35 of 2004**

1. On 17 August 2006 the Constitutional Court ruled that the above Act is inconsistent with the Constitution and therefore invalid. The order declaring it invalid has been suspended for 18 months to enable Parliament to enact this statute afresh in a manner that is consistent with the Constitution.
2. Once the above Act has been promulgated, due regard will have to be given in terms of the imposition of confidentiality provisions on traditional health practitioners.

Q. Patients' Rights Charter

1. The Department of Health published the Patients' Rights Charter during 2002. This document spells out the **rights and responsibilities of patients** in terms of health care.
2. The Department of Health has proclaimed the Patients' Rights Charter as a common standard for achieving the realisation of the **right of access to health care services** as set out in the Constitution of the RSA.
3. It is to be noted that this Charter is subject to the provisions of any law operating within the RSA and to the financial means of the country.
4. This Charter provides that information concerning a person's health, including information concerning treatment, may only be disclosed with **informed consent**, except when required in terms of **any law** or **an order of the court**.
5. Insofar as informed consent is concerned, the Charter stipulates that everyone has the right to be given **full and accurate information** about the nature of one's illnesses, diagnostic procedures, the proposed treatment and the costs involved, for one to make a decision that affects any one of these elements.
6. In particular, this Charter lists the respective responsibilities of the patient. The responsibilities that are applicable to this report are that every patient must:
 - 6.1. enquire about the related costs of treatment and/or rehabilitation and arrange for payment;
 - 6.2. take care of health records in his or her possession;
 - 6.3. respect the rights of other patients and health care providers; and
 - 6.4. provide health care providers with the relevant and accurate information for diagnostic, treatment, rehabilitation or counselling purposes.

X. INFORMED CONSENT FOR SUBMISSION OF PERSONAL HEALTH INFORMATION

1. As set out in **Chapter IX** above, the health care provider must obtain informed consent from the patient. For purposes of this document, the reader must distinguish between consent for treatment as envisaged in the NHA and consent by the patient for the submission of PHI.
2. In terms of the **Protection of Personal Information Bill** “consent” is defined as **any freely-given, specific and informed expression of will** whereby data subjects agree to the processing of personal information relating to them. This Bill also requires that personal information must be collected for a **specific, explicitly defined and legitimate purpose**.
3. The ECT Act relates to instances where a data controller must have the **express written permission** of the data subject.
4. Section 7 of the NHA only relates to obtaining informed consent from a user for the provision of a specified **health service**. This consent therefore only relates to treatment and not to the submission of PHI such as ICD-10 codes *per se*.
5. In the case of an emergency, it is proposed that should the disclosure of PHI be required, sections 6, 7, 8 and 9 of the NHA should be followed *mutatis mutandis*.
6. Having regard to the regulatory framework as documented in **Chapter IX**, it is clear that to enable a patient to grant informed consent for the submission of PHI, the following information must be given to the patient:
 - 6.1. the reasons / purposes for the disclosure;
 - 6.2. the likely consequences of disclosure;
 - 6.3. the intended recipients of the PHI; and
 - 6.4. the likely consequences of non-disclosure if the patient is entitled to medical scheme benefits, namely that the medical scheme may elect not to reimburse the claim of the patient.
7. Health care providers have obligations towards patients who may be beneficiaries in procuring informed consent for the submission of PHI whereas medical schemes have obligations towards beneficiaries in procuring informed consent for the submission of PHI. It is to be considered what the respective obligations of health care providers and medical schemes are in this regard.

8. **The following submission was made by the HPCSA in its capacity as a participant in this consultative process in respect of Informed Consent as viewed by the HPCSA:**

8.1. **Definition**

Informed consent is an exercise of an **informed choice** by a patient who **has the capacity** to give consent:

- 8.1.1. in instances where there are multiple options or alternatives to treatment; or
- 8.1.2. in making a decision whether to withhold or disclose information or allow someone else to disclose information on their medical condition to a defined third party; or
- 8.1.3. in making a decision for purposes of reimbursement by a Medical Scheme,

based on adequate information and a detailed analysis or unpacking of each of the options or alternatives as well as the legislative requirements for disclosure of such information.

This means there must be a full and frank disclosure of all the material facts to enable the patient decisions from an informed basis. With regards to PHI, for instance, the patient should be given information as to who will access their information, for what purpose and what would be the implications of the utilization of such information etc.

8.2. **Health Care Provider Responsibilities: PHI**

Health care providers have the following obligations, the list not being exhaustive as any other ethical obligation in handling and dealing with patient information and respecting their confidentiality will be required:-

- 8.2.1. to provide information to the patients about the legislative requirement of supplying ICD-10 codes to the medical schemes for purposes of reimbursements and the inevitable consequences of the medical scheme becoming aware of the diagnosis of the patient/member;
- 8.2.2. to procure patient consent to release ICD-10 coding to the medical scheme and/or (where required) to the other health care provider (within the health care team);
- 8.2.3. to advise the patient of their choice not to have their ICD-10 coding divulged to the medical scheme which would mean the patient has to settle the health care provider's account directly; and
- 8.2.4. to indicate that the practitioner does not have control over the management and utilization of this information once divulged over to the medical scheme and that the medical scheme takes responsibility for any further disclosure or utilization of such information for whatever purpose.

It is strongly suggested that written consent be procured from the patients by the health care providers in order to safeguard the interests of both parties. Consent by a patient may be once-off in relation to the treatment of a similar condition provided there is a verbal reminder to the patient about their initial commitment to confirm if they are still comfortable with the disclosure. It would be advisable for a health care provider to note the verbal reminder on that patient's file. Where a patient presents with a new or different condition, a fresh consent should be obtained from the patient and appropriately documented.

Health care providers without direct patient contact like pathologists and radiologists act on referrals from other health care providers. Their responsibility would be to ensure that the referring health care provider has procured consent for him/her (in this case a pathologist or radiologist) to access and also disclose the information to the medical scheme for reimbursement purposes.

8.3. **Informed Consent for Inter-Council Interaction of health care providers as Members of a Health Care Team**

Sharing of information with members of a health care team providing a health service to a patient would be permissible to the extent that it is necessary to enhance the quality of care to be provided to that patient and the patient has given consent to treatment and disclosure of such information to another health care provider. This would include members beyond the HPCSA.

9. It is recommended that the respective Professional Councils acting in accordance with their own discretion should develop a *pro forma* informed consent together with ethical rules or guidelines for the disclosure of PHI by their respective members. The Subcommittee has drafted a **pro forma consent** (see Annexure "A" in this regard) to be used as a basis for reference by the respective Professional Councils who in their discretion should adapt this proposed consent to cater for the needs of the respective health care providers in line with applicable legislation and ethical rulings pertaining to such health care providers.

XI. INFORMATION SECURITY

1. Introduction

1.1 Three important principles govern information security, namely:

1.1.1 **Confidentiality:** No unauthorised person must have **access** to PHI;

1.1.2 **Integrity:** No unauthorised person can **amend** PHI; and

1.1.3 **Availability:** All authorised persons must have **access** to PHI that they need.

1.2 **Authorised** in the context of this document will translate to “**Informed Consent**”.

1.3 Section 17 (1) of the **Protection of Personal Information Bill** provides that the responsible party must implement **appropriate technical & organisational measures** to secure:

1.3.1 the **integrity** of personal information by safeguarding it against the **risk of loss or damage**;

1.3.2 against the **unauthorised or unlawful access** to or **processing of personal information**.

1.4 Section 17 (2) of the **Protection of Personal Information Bill** provides further that the responsible party must take **measures** to:

1.4.1 identify all reasonable foreseeable **internal and external threats** to personal information;

1.4.2 maintain **appropriate safeguards**;

1.4.3 regularly verify that the safeguards are **effectively implemented**; and

1.4.4 update safeguards in response to **new risks** or **deficiencies** in previously implemented safeguards.

1.5 To comply with the above it is contended that a responsible party must have due regard for **generally accepted practices and procedures** relating to personal health information security.

2. ISO Standards Documents related to Confidentiality of Patient Data

2.1. Introduction

This summary of ISO (International Organization for Standardization) documents relevant to the confidentiality of patient data is intended to complement the publication of a report, under the auspices of the ICD-10 Implementation Task Team, on confidentiality aspects of the implementation of ICD-10 as the South African national standard for diagnosis coding.

Significant work on the development of relevant standards has already taken place, and is in progress, in the ISO technical committee on Health Informatics (ISO/TC 215 Health Informatics). The aim of this document is to highlight existing and developing standards which could be taken into account in the development of policies and practices to ensure the maintenance of patient confidentiality in health information systems and in the exchange of patient information between stakeholders in South Africa.

Some of the ISO documents referred to in this report have not yet been finalised, and may therefore not be formally referenced in legislation or policy documents. However, these documents are very relevant to the ICD-10 implementation, and should therefore be taken into account in the development of policy. South Africa, as a P (participating) member of ISO/TC 215, has the opportunity to influence the content to ensure that the needs of the South African community are taken into account in the final versions.

Several of the relevant ISO standards have been adopted as South African national standards, and are therefore available as publications of the South African Bureau of Standards (SABS).

2.2. ISO and SABS Standards

- 2.2.1. A list of ISO and SABS standards which should be taken into account in the implementation of ICD-10 as the national standard for diagnosis coding is attached as Annexure B.
- 2.2.2. One of the key issues related to patient confidentiality is that patients and health care providers need to be confident that patient data will be handled appropriately both within organisations and, as is very often the case, when data is transferred between organisations and/or health care providers and/or other stakeholders. ISO/TC 215 continues to address the issue of health information security through its Working Group 4 (Security). The issues related to maintaining the security of patient data therefore relate to all aspects of patient data, including data coded using ICD-10 or other coding systems.
- 2.2.3. The ISO standard which relates to the code of practice for information security management (ISO/IEC 17799 / SANS 17799:2005 Information Technology – Security techniques – Code of practice for information security management) has already been adopted as a national standard. IT Security has been identified as one of the key strategic focus areas of SITA, the State IT Agency, as stated in the SITA Procurement Policy and Procedures (SITA, 2002). Among the requirements for certification of IT solutions by SITA is compliance with ISO 17799. **Compliance with SANS 17799 should be a basic requirement for all electronic information systems which handle patient data.**

- 2.2.4. ISO/TC 215 is developing standard 27799 (ISO/DIS 27799 Health Informatics – Security management in health using ISO/IEC 17799) to address additional information security management requirements for the health domain. **Once it has been finalised, compliance with ISO 27799 should be a further requirement for all electronic information systems which handle patient data. A summary of some aspects of information security covered by ISO/DIS 27799 is attached as Annexure C.**
- 2.2.5. The ISO standard on data protection to facilitate trans-border flows of personal health information (ISO 22857) could also be applied to flows of personal health information between organisations, as is often required. This standard provides some very practical guidelines for maintaining patient confidentiality. **Compliance with the appropriate components of ISO 22857 could greatly enhance user confidence that patient data is being handled confidentially at all stages in the information flow process. A summary of some aspects of information security covered by ISO 22857 is attached as Annexure D.**
- 2.2.6. The national ID number is currently used as the patient ID in computerised health information systems. This constitutes a very serious risk to patient confidentiality, especially in the context of exchange of patient data between parties. Serious consideration needs to be given to the development of an alternate patient identifier, possibly based on a one-way encryption of the ID number using a PKI (Public Key Infrastructure) approach. The implementation of the smart card-based pensions system by the SAPO makes use of PKI, with the Post Office as the Trusted Third Party (TTP) for handling the keys. **SA national standards in the form of a Technical Specification on PKI for health have been defined, using the corresponding ISO standards. (SANS 17090-2003 / ISO/TS 170909-2002: Health Informatics – Public Key Infrastructure; 3 parts).**
- 2.2.7. The ISO Technical Report on trusted end-to-end information flow (ISO/TR 21089) 'offers recommendations on best practice' for a wide range of stakeholders, including patients. It provides information to support tracing and auditing of information flows at identified 'key trace points' for patient records.
- 2.2.8. A technical specification is being developed on Pseudonymisation, the process of de-identifying personal data in such a way that information may be linked to the same person across multiple records without revealing the identity of the specific person to whom the data refer (Health Informatics – Pseudonymisation practices for the protection of personal health information and health related services). This document, when published, will provide valuable practical guidelines for ensuring the secure handling of patient data, even when data on a particular patient needs to be linked for various applications.

2.2.9. ISO/TC 215 (Health Informatics) has developed and is developing multiple standards related to the exchange of patient data between multiple parties. **A comprehensive list of the standards and projects of ISO/TC215, and related SA standards, has been provided by SABS and is attached as Annexure B. Document numbers which include 'D' and do not include a date are standards that have not yet been finalised.**

3. Conclusion

- 3.1 It is to be noted that information security is a **legal obligation**.
- 3.2 One of the key barriers to the exchange of patient data between parties, even for legitimate reasons, is the perception among health care providers and patients that the confidentiality of the data could be compromised in the process of data exchange.
- 3.3 **Policies and procedures** therefore need to be implemented, and be seen to be implemented, which are designed to ensure the confidentiality of patient data at all stages of processing, storage and use.
- 3.4 The implementation of **appropriate national and international standards** designed to address the issue of confidentiality will be an important component of ensuring the confidentiality of patient data and other related data.

XII. PROTECTION OF PERSONAL HEALTH INFORMATION WITHIN DATA MANAGEMENT COMPANIES

1. For this Chapter of the report:
 - 1.1. switching companies, data management / data transfer companies and any other entity switching or processing PHI constitute “data management companies”;
 - 1.2. medical schemes, medical scheme administrators and managed care organisations that are accredited by the Council for Medical Schemes are excluded from the definition of “data management companies”.
2. Although data management companies may constitute **data controllers** as defined in the ECT Act that are therefore subject to the provisions of the ECT Act, there are qualifications as set out in the ECT Act to the regulation of these entities.
3. Under the current legal dispensation there is no regulatory body to oversee the activities of these companies.
4. The Patient Confidentiality Subcommittee initiated discussions with data management companies that were prepared to assist with this consultative process. The Code of Conduct and Mission Statement set out in Annexures E and F were voluntarily proposed by these data management companies in the absence of a regulatory body that oversees the activities of these companies.
5. It is therefore proposed that any entity switching or processing PHI as per **paragraph 1.1** above subscribe to a code of conduct as set out in Annexure E to ensure the integrity, privacy, confidentiality and security of PHI.

XIII. RECOMMENDATIONS

1. Introduction

The recommendations set out below are made in addition to the existing regulatory and ethical framework as documented under [Chapter IX](#) to ensure that role players in the health care industry have appropriate and effective safeguards in place to ensure the protection of patients' personal health information.

2. General Recommendations

- 2.1. Patient data, including ICD-10 diagnostic codes that are to be used for **research, training, education or benchmarking** purposes should be **de-identified or anonymised** as soon as identifiable information is no longer required along the data chain / information pathway.
- 2.2. Where appropriate, role players in the health care industry should **develop or review codes of conduct, policies and standard operating procedures** that cater for privacy and confidentiality and in particular, the use of personal health information.
- 2.3. Employees of all role players in the health care industry should be **trained** on the legal and ethical requirements of the protection of personal health information.
- 2.4. Employees of all role players in the health care industry should sign **confidentiality agreements**.
- 2.5. A breach of patient confidentiality should be included as a **disciplinary offence** in the **code of conduct** for all role players in the health care industry.
- 2.6. System applications should have the **capability of setting access rights** so that an employee only has access to the information that he or she requires.
- 2.7. In general, employees must be aware that they only have access to personal health information on a "**need to know**" basis.
- 2.8. System applications must have **adequate audit and control functions**. Audit trails should be reviewed regularly and their existence should be communicated.
- 2.9. System applications should be programmed to log people off after a specified period of inactivity. Alternatively, employees should be required to use **password protection** on screen savers. A recommended period in a high traffic area is 5 minutes.

- 2.10. Policies should be established to immediately withdraw a terminated employee's access to patient information. It is strongly suggested that those employees who worked closely with the former employee should also have their passwords reset as these may also have been compromised.
- 2.11. Policies should be established on network and application password controls. This policy should cover how often network and application passwords should be changed.
- 2.12. Information provided to a **legal representative or debt collection agency** acting on behalf of a health care provider, medical scheme, medical scheme administrator or managed care organisation should not include personal health information. Only the quantum and cause of action should be disclosed. The nature and extent of the treatment, including any diagnostic information such as ICD-10 codes, should only be disclosed where this is pertinent to the dispute and then only if raised by the patient in question.
- 2.13. As laws and their implementation can be subjected to constitutional scrutiny, the **purpose of disclosure** of personal health information such as ICD-10 codes should be clear.
- 2.14. According to CMS Circular 33 of 2006 dated 25 July 2006, **ICD-10 codes for non-disclosure of clinical information** are valid and cannot be rejected by medical schemes on this ground alone, although this may impact on reimbursement. These non-disclosure codes are:
 - 2.14.1. U 98.0 : Patient refusal to disclose clinical information;
 - 2.14.2. U 98.1 : Service provider refusal to disclose clinical information.

Patients should be informed that the use of the above codes may result in either the medical scheme electing to pay the claim from day-to-day / acute benefits, or electing to pay the claims from the member's savings account or electing to reject the claim. It is in the discretion of the medical scheme to decide how to proceed when these codes are submitted.
- 2.15. All role players in the health care industry should **regularly review their risks** relating to **information security** such as:
 - 2.15.1. physical and operational risks;
 - 2.15.2. human resource risks;
 - 2.15.3. technology risks;
 - 2.15.4. business continuity and disaster recovery risks;
 - 2.15.5. compliance with legislation and acknowledged national and international standards.
- 2.16. **Students** that are still studying to become health care providers should be taught of the importance and all aspects of the protection of personal health information as part of their *curriculum*.

- 2.17. It is proposed that any company **switching or processing personal health information** as defined in **Chapter XII** subscribe to a **code of conduct** to ensure the integrity, privacy, confidentiality and security of personal health information.
- 2.18. It is proposed that the Department of Health as part of its strategy for the National Health Information System adopt **confidentiality and security standards for the health care industry**.
- 2.19. The Department of Health should educate the public regarding the disclosure of personal health information.

3. **Health Care Provider Specific Recommendations**

- 3.1. Notwithstanding the provisions of the General Recommendations, Health care providers should:
 - 3.1.1. take appropriate action to protect the privacy of all patients, including minors;
 - 3.1.2. set up control measures to prevent unauthorised access to personal health information;
 - 3.1.3. obtain written informed consent from the patient or other legally authorised person for the disclosure of personal health information such as ICD-10 codes;
 - 3.1.4. consider displaying visible notices in their waiting room regarding the use of personal health information such as ICD-10 codes on accounts;
 - 3.1.5. conclude confidentiality and non-disclosure agreements with third party service providers;
 - 3.1.6. make patients aware that personal health information will be shared within the health care team to ensure the continuity of care, unless patients object.

4. **Medical Scheme, Medical Scheme Administrator and Managed Care Organisation Specific Recommendations**

Notwithstanding the provisions of the General Recommendations,

- 4.1. Medical scheme contracts with members should state the reasons for disclosure of personal health information such as ICD-10 codes, the likely consequences of disclosure as well as non-disclosure and the intended recipients of personal health information such as ICD-10 codes.

- 4.2. Medical schemes should review their policies to extend its membership contract to dependants of consenting age.
- 4.3. There is a need for medical schemes to contract with all their third party service providers to ensure the protection of the confidentiality of PHI. This view is also supported by the CMS in its document titled "Putting Members First: Towards Better Governance of Medical Schemes - Findings and Recommendations of the Governance Theme Project" dated May 2006.⁸⁸
- 4.4. There should be ongoing education of medical scheme members regarding the purpose and intended recipients of personal health information such as ICD-10 codes. Medical schemes will have to educate their members in accordance with the "Notice to Consumers: ICD-10 Coding: All you need to know as a consumer" as published by the CMS on 9 February 2007.
- 4.5. Medical schemes should review access to personal health information of dependants by members, e.g. website access, information printed on member statements, etc.
- 4.6. Medical schemes or their administrators must review call centre procedures relating to the disclosure of personal health information such as ICD-10 codes.

5. Professional Council Specific Recommendations

Notwithstanding the provisions of the General Recommendations,

- 5.1. It is recommended that the respective Professional Councils acting in accordance with their own discretion should develop a *pro forma* informed consent together with ethical rules or guidelines for the disclosure of PHI by their respective members. The Subcommittee has drafted a **pro forma consent**, as set out in paragraph 9 of Chapter X, to be used as a basis for reference by the respective Professional Councils who in their discretion should adapt this proposed consent to cater for the needs of the respective health care providers in line with applicable legislation and ethical rulings pertaining to such health care providers.
- 5.2. The respective Professional Councils should also issue guidelines on how often a signed consent should be obtained by the health care provider and the period for which a signed consent, once obtained, will be valid.

6. Council for Medical Scheme Specific Recommendations

Notwithstanding the provisions of the General Recommendations,

- 6.1. The CMS may have to consider changes to the MSA depending on the intended use of personal health information such as ICD-10 codes. This is critical as a patient should be guaranteed that their personal health information will only be used for those reasons for which they gave informed consent.

⁸⁸ The report can be found at <http://www.medicalschemes.com/Publications/Publications.aspx?catid=3>

- 6.2. The CMS should ensure that all medical schemes, as part of the **accreditation process**, have evidence of contractual agreements with third party service providers, including but not limited to data management companies.
- 6.3. The CMS should consider reviewing the **accreditation standards for brokers** to ensure the protection of PHI.
- 6.4. The CMS should monitor **compliance with accreditation standards of Administrators, Managed Care entities and Brokers** set for the protection of personal health information and should consider conducting random audits in this regard.
- 6.5. A list of all data management companies that have agreed in writing to adhere to the Code of Conduct and Mission Statement of the South African Health Care Data Management Society should be published on the website of the CMS.
- 6.6. CMS should ensure the protection of personal health information with regards to data collected, e.g. Statutory returns, Risk Equalisation Fund.

XIV. CONCLUSION

1. Health care providers must obtain **informed written consent** from the patient or legal authorised person in order to comply with regulation 5(f) of the MSA when including a diagnostic code such as ICD-10 and other codes on an account to be submitted to a medical scheme, as well as when using such codes to communicate with the other members of the health care team through prescriptions, pathology requests, radiology requests, hospital discharge summaries and the like.
2. It is to be noted that **patient confidentiality and information security are legal obligations**.
3. Although there is already an **adequate regulatory framework** in place to protect personal health information, **further recommendations** have been suggested to **improve the level of compliance** towards maintaining the privacy, confidentiality, security and integrity of personal health information.
4. Until the Protection of Personal Information Bill is promulgated, it is recommended that health care providers and medical schemes conclude written agreements with third party service providers to ensure that personal health information is protected.

XV. ANNEXURES

ANNEXURE A: Pro Forma Informed Consent for Health Care Providers

All health care providers in South Africa are required by law, to include diagnosis and treatment information in the form of ICD-10 and other codes on all claims or accounts. This applies to all claims that are submitted directly to medical schemes by doctors and other health care providers, or accounts paid directly by the member/beneficiary to the health care provider and which are then claimed back from the medical scheme.

These diagnosis and treatment codes provide accurate information on your health condition and thereby help your Medical Scheme to determine what benefits you are entitled to and how the benefits can be paid.

In order to promote and ensure the continuity of your care, diagnosis and other codes are also required on medicine prescriptions, on hospital discharge summaries and referral notes to other members of your Health Care Team.

The informed consent form, below, allows you to indicate whether you either want to give consent or refuse consent to submit your private health information to your medical scheme for accurate payment of your claims and to other members of your health care team for further treatment.

You have the right to decide that you do not want to disclose your private health information to your medical scheme or to the other members of the Health Care Team. In this case a non-disclosure code (i.e. U98.0 - patient refused to disclose clinical information) will be used. However, when this code is used, you should be aware of the following:

- Your medical scheme is not obliged to pay the claim/account as they need your health information (such as ICD-10 codes) in order to do so.
- Your medical scheme may not pay for the services rendered and you will be liable for the account.

You have the right to withdraw any consent given or refused at any future visit. Should this occur, you will need to inform me of this decision and sign another informed consent form, indicating your amended decision.

I confirm that I understand the above information and I have exercised my choice voluntarily.

I hereby **grant** consent to _____ (name of health care provider) to submit my personal health information as described above.

I hereby **do not grant** consent to _____ (name of health care provider) to submit my personal health information as described above.

Patient's (or Legal Guardian's) full name (in print): _____

Patient's (or Legal Guardian's) signature: _____

Date (dd/mm/yyyy): _____

ANNEXURE B: ISO and SABS Standards relevant to the Implementation of ICD-10 and other Codes as the South African National Standard for Diagnosis Coding

SANS 17799: 2005	ISO/IEC 17799: 2005	Information Technology – Security techniques – Code of practice for information security management, 2005	
In draft – under discussion	ISO/DIS 27799	Health Informatics – Security Management in Health using ISO/IEC 17799	Currently out to ballot as an international standard
In draft – under discussion	ISO 22857: 2004	Health Informatics – Guidelines on data protection to facilitate trans-border flows of personal health information	
SANS 17090-1:2003	ISO/TS 17090 – 1:2002	Health Informatics – Public key infrastructure Part 1: Framework and overview	ISO Technical Specification
SANS 17090-2:2003	ISO/TS 17090 – 2:2002	Health Informatics – Public key infrastructure Part 2: Certificate profile	
SANS 17090-3:2003	ISO/TS 17090 – 3:2002	Health Informatics – Public key infrastructure Part 3: Policy management of certification authority	
In draft – under discussion	ISO/TR 21089: 2004	Health Informatics – Trusted end-to-end information flows	ISO Technical Report
SANS 17090-2:2003	ISO/TS 17090 – 2:2002	Health Informatics – Public key infrastructure Part 2: Certificate profile	
SANS 17090-3:2003	ISO/TS 17090 – 3:2002	Health Informatics – Public key infrastructure Part 3: Policy management of certification authority	
In draft – under discussion	ISO/TR 21089: 2004	Health Informatics – Trusted end-to-end information flows	ISO Technical Report

ANNEXURE C: Comments on ISO/DIS 27799: Health Informatics – Security Management in Health using ISO/IEC 17799

ISO 27799 promises to be a very practically-orientated document, as is ISO/IEC 17799, designed to facilitate the implementation of special measures related to the secure handling of personal health information. The provisions of ISO 27799 are complementary to those of ISO/IEC 17799, which means that the two standards should be implemented together.

The ISO 27799 document notes that South Africa is among the countries which are already using ISO/IEC 17799 for health informatics security management.

In section 5.1, the document states that 'Maintaining information confidentiality, availability and integrity (including authenticity, accountability and auditability) are the overarching goals of information security. In health care, patient privacy depends upon maintaining the confidentiality of personal health information.'

In section 5.4, it is noted that **the following types of health information need to be protected:**

- personal health information
- pseudonymised data derived from personal health information via some methodology for pseudonymous identification
- statistical and research data, including anonymised data derived from personal health information by removal of personally identifying data
- clinical/medical knowledge not related to a specific patient or patients, including clinical decision support data (e.g. data on adverse drug reactions)
- data on health care providers and staff
- information related to public health surveillance
- audit trail data that are produced by health information systems containing personal health information or pseudonymous data derived from personal health information or data about the actions of users in regard to personal health information, and
- system security data, including access control data and other security related system configuration data, for health information systems.

It is noted that 'the extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed', making the important point that one size does not fit all in this context.

The implementation of a comprehensive and cohesive Information Security Management System is recommended, supported by the demonstrated and active support of management, which is an essential prerequisite for success.

Section 7, the largest section of the document, 'contains **specific advice on the eleven security control clauses and 39 main security control categories**' in ISO/IEC 17799 (and therefore in SANS 17799). The topics covered in section 7 are:

- information security policy
- organising information security
- asset management
- human resources security

- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance.

Section 7.2.1.3 refers to **confidentiality agreements**, highlighting the fact that

In addition to following the guidance given by ISO/IEC 17799, organisations processing personal health information shall have a confidentiality agreement in place that specifies the confidential nature of this information. The agreement shall be applicable to all personnel accessing health information.

Section 7.3.2 **Health Information Classification** recommends that 'organisations processing personal health information should uniformly classify such data as confidential' and ensure that all printed and electronic documents which include personal health information must be marked confidential.

The document will include informative annexures (i.e. not implementable as part of the standard) on threats to health information security; tasks and related documents of the Information Security Management System, and potential benefits and required attributes of support tools, as well as a list of related standards in health information security.

ANNEXURE D: Comments on ISO 22857: Health Informatics – Guidelines on Data Protection to Facilitate Trans-Border Flows of Personal Health Information

ISO/DIS 27799 notes in section 7.2.2.3 that 'where information flow crosses jurisdictional boundaries, additional guidance can be found in ISO 22857'. This situation is especially applicable in situations of sharing data between health care providers, and between health care providers and other organisations, such as medical schemes, medical scheme administrators and managed care organisations.

Among the issues highlighted in this standard are the following:

- identification of 'appropriate' and 'required' levels of security measures, based on an assessment of potential risk;
- the need for 'adequate' data protection;
- data must only be transferred for specific purposes;
- data subjects (i.e. the persons to whom specific data refers) must be identified for no longer than is necessary for the purposes for which the data were transferred;
- data subjects have the right to access data being held about them, and rectify the data if necessary;
- anonymisation of data prior to transfer is recommended;
- measures must be defined for dealing with secondary use of data; and
- the need to be able to identify very sensitive data, in consultation with data subjects, and implement additional controls in order to ensure the confidentiality of such data.

ANNEXURE E: Code of Conduct for Data Management Companies as proposed by Members of the South African Health Care Data Management Society

1. Members of the South African Health Care Data Management Society shall strive to provide the highest standard of professional conduct, thereby ensuring that health care data is managed and transported confidentially and securely with regards to individual patient-identifiable data.
2. Members shall respect the rights of patients, physicians and colleagues in the health care industry and will ensure that the data of patients is not manipulated, and that identifiable data is used only for the original purpose it was intended for.
3. Members shall use only legal and ethical means in all professional dealings with individual identifiable data and will refuse to cooperate with or condone by silence the action of those who engage in fraudulent, deceptive or illegal acts.
4. Members shall respect the laws and regulations of the Republic of South Africa, and uphold the mission statement of the South African Health Care Data Management Society.

ANNEXURE F: Mission Statement of Data Management Companies as proposed by Members of the South African Health Care Data Management Society

1. As a health information data management company, I will equip myself with appropriate safeguards based on Industry Best Practice, e.g. encryption, message authentication and user verification, to protect the privacy of physician and patient-identifiable information.
2. The staff and/or contractors in my service are subject to clear, explicit and mandatory policies and procedures regarding the entry, management, storage, transmission and distribution of patients' identifiable information.

This Code of Conduct strives to promote and maintain the highest standard of professional conduct amongst its members. Adherence to these standards is based on public confidence and the integrity of Health Care Data Management companies. Failure to adhere to these standards may result in the loss of credentials and membership of the Health Care Data Management Society.

Membership Information to be placed in Public Domain

By agreeing to adhere to the above Code of Conduct and Mission Statement, members of the South African Health Care Data Management Society also agree that it may be made public that they are members of this Society.