

GUIDING PRINCIPLES ON PRIVACY AND CONFIDENTIALITY

EXECUTIVE SUMMARY

This document contains a Definitions Clause and the 14 guiding principles relating to privacy and data-protection as it pertains to the health funding area. These are:

1. [Adherence to legislation governing rights to privacy and confidentiality](#)
2. [Anonymisation of data](#)
3. [Privacy protection should follow data, as- and where it flows](#)
4. [People have access to their own information held by third parties](#)
5. [Health care roleplayers should establish privacy policies and procedures](#)
6. [Notification to persons on uses of their information](#)
7. [The applicable ISO standard to be adhered to in cross-border transfer of data](#)
8. [Disclosure of information may only take place on authorisation by a law, a court of law or with written consent of the person](#)
9. [Financial or organisational links do not permit free flow of personal information](#)
10. [International standards and local legislation and policy should be adhered to in cases of research](#)
11. [Disclosures to law enforcement officials should not take place outside of the applicable legal requirements](#)
12. [Non-discrimination principles, as enshrined in PEPUDA and the EEA should be adhered to](#)
13. [Employee contracts should include provisions on confidentiality](#)
14. [Stakeholders should be held accountability for breaches of information](#)

Since these principles were written and proposed, various events have coloured both law and politics concerning the right to privacy and data, including the promulgation of the National Health Act, the SA Law Commission Issue Paper on Privacy and Data-protection and the controversy relating to the sale of data for commercial purposes, sparked by the alleged Post Office sale of addresses. It is suggested that the Electronic communications and transactions Act of 2002 also be considered in more detail, including the provisions on voluntary adherence to data-protection principles.

Moreover, in the health care funding industry health data no longer only relates to "whether to pay or not", but also to "whether to intervene/manage or not". Furthermore, risk calculations may still be bound to health data relating to current and past medical scheme members (within a particular scheme or within a particular group of schemes), requiring access to as comprehensive a health care picture as possible. Proposals in terms of a social health insurance system may affect the basis on which data is collected, from whom it is collected and the purposes for which it is used.

Until data-legislation is passed, interim measures have to be instituted in line with applicable legislation and general constitutional principles.

DEFINITIONS

“Anonymised data” means data from which the patient cannot be identified by the recipient of the information. The name, address, and full postal code must be removed, together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the patient. Patient reference numbers or other unique numbers may be included only if recipients of the data do not have access to the 'key' to trace the identity of the patient using that number.

“Consent” means an agreement to an action based on knowledge of what the action involves and its likely consequences.

“Critical data” means data that is declared by the Minister in terms of section 53 of the Electronic Communications and Transactions Act No. 25 of 2002, to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens.

“Critical database” means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted.

“Express consent” means consent which is expressed orally or in writing (except where patients cannot write or speak, when other forms of communication may be sufficient).

“Generic” means that the standards' requirements can be applied to any organisation.

“Health care team” means the health care team who comprise the people providing clinical services for each patient and the administrative staff who directly support those services.

"Health care role player" refers to medical schemes, administrators, managed care organisations, service providers, intermediaries and their employees, governing bodies, trustees and Boards of Directors.

“Patients” means competent patients and parents of, or those with parental responsibility for, children who lack maturity to make decisions for themselves. (Adult patients who lack the capacity to consent have the right to have their confidentiality

respected. Guidance on disclosure of information about such patients is included in paragraph 5.4 hereof.)

“Personal information” means information about people which doctors learn in a professional capacity and from which individuals can be identified.

“Personal- or health information” refers to all information that is personal or could be re-linked to a particular person or group and that pertains to the health and/or health care, treatment, diagnosis, tests, procedures, stay in health care facilities, and any other related health care information of any person or group. It includes any record that contains these types of information, irrespective of its format or type.

“Public interest” means the interest of the community as a whole, or a group within the community or individuals.

“Standards” refers to documented agreements containing technical specifications or other precise criteria to be used consistently as rules guidelines or definitions or characteristics to ensure that materials, products, process and services are fit for their purposes.

GUIDING PRINCIPLES

Principle 1: All parties dealing with patient health care and personal information have to take into account relevant legislation, such as the Constitution of the RSA of 1996, the Medical Schemes Act of 1998, the Promotion of Access to Information Act of 2000, the National Health Act of 2003 and specific provisions contained in health- and health care legislation.

Principle 1.1: Information may be disclosed by a service provider to a medical scheme in execution of a managed care agreement as provided for in the regulations to the Medical Schemes Act of 1998. Where such disclosure is made to an administrator or any third party on the basis of a contract between the scheme and such administrator or third party in terms of this specific regulation, the administrator or third party is bound by the same provisions as the scheme. Access to patient information is limited in scope by the exact provisions of the contract between the managed care organisation and the scheme and the *purpose* for which the information is provided, e.g. evaluation of benefits, motivation for pre-authorisation, etc. This information should not be passed on to any other department within that organisation,

scheme or administrator which does not deal with managed care. This information should also not be used to risk-rate a particular patient/member/dependant and/or to reduce benefit levels that would have been different in the absence of such information.

Disclosure of personal or health Information may be refused if it is requested for "random audits of practices", to include on health databases or practice profiling (if the practice profiling does not focus on affordability and appropriateness of care, or as a risk management tool in accordance with an agreement entered into in terms of Regulation 15A of the Medical Schemes Act Regulations, but is required only for financial benchmarks).

Principle 1.2: Administrators and intermediaries are obliged to keep confidential all information and material in their possession and relating to its duties *vis á vis* a medical scheme and/or service provider; and *are* bound by the same principles governing the conduct of the scheme and/or service provider in relation to patient information confidentiality and disclosure.

Principle 1.3: Any third party request for information is to be dealt with in terms of the Promotion of Access to Information Act of 2000. The provisions of Section 15 and 16 of the National Health Act should also be adhered to.

Principle 1.4: All coded data on accounts by service providers' *vis-à-vis* specific aspects of confidentiality falls outside the scope of these general principles.

Principle 2: For all uses and disclosures of health information all "health care role players" should remove personal identifiers consistent with maintaining the usefulness of the information, unless legislation authorises specific personalised disclosures. Nothing prevents the compilation and/or manipulation of anonymous information for the purposes of financial- or other planning, for risk calculation within the scope as permitted by legislation or for statistical purposes, related to the core business of the entity in possession of the information. The role player compiling and/or manipulating such information lawfully owns such information.

Principle 3: Privacy protections should follow the data, irrespective of the number of intermediaries between the patient, as initial provider of the information, and any final destination. This also applies to electronic messaging.

3.1 Section 17 of the National Health Act places a duty on health establishments to ensure that there is no unauthorised access to records, which implies the setting up of mechanisms to verify record and data requests, even where these are from funding institutions or data warehouses. Failure to do so constitutes an offence under the Act.

3.2 The onus of protecting confidential information vests with the holder thereof. Health care role players should, therefore, implement security safeguards for the storage, use, and disclosure of health information, irrespective of the format of such information. Confidentiality agreements should also be entered into with third parties to whom information is disclosed beyond the extent of the principles herein contained.

3.3 Health information handed over to an attorney or debt collection agent for legal proceedings should not include medical records, i.e. only the quantum and course of action should be disclosed. The nature and extent of treatment would only be raised should there be a dispute to which this information is pertinent and if such is raised by the patient him/herself.

Principle 4: An individual *has* the right to access his or her own health information, as regulated by the Promotion of Access to Information Act of 2000 and other relevant legislation, and the right to supplement such information.

In terms of the National Health Act a person's right to know his or her health status may be withheld "in circumstances where there is substantial evidence that the disclosure of the user's health status would be contrary to the best interests of the user". This section gives statutory recognition to the common law doctrine of therapeutic privilege.

Principle 5: Health care role players should, in effecting their duties in terms of section 57(4)(i) of the Medical Schemes Act, establish policies, procedures and review mechanisms regarding the protection of confidentiality, as well as the collection, use, and disclosure of health information.

Principle 6: Individuals should be given notice about the (possible) uses-, purposes- and disclosures of their health information in the chain of health care and health care financing, even where such information would be anonymised. Individuals have to be informed about their rights with regard to that information. This should be done at the point of potential delivery of health care, as well as the point of application for medical scheme membership or health insurance.

6.1 In order for members/patients to have control over their information, they should at some point consent to the variety of uses to which their information may be put.

6.2 Cognisance should be taken of the provision of section 52ff to the Electronic Communications and Transactions Act of 2002, whereby some databases may be declared "critical databases" and certain measures have to be instituted to secure the database and access to it.

Principle 7:

Personal health information on users may be transferred across national borders and collected, stored, processed, and published for many purposes, including clinical research and health statistics. Since the extent of the protection afforded to personal health data varies from country to country, the common and internationally accepted ISO International Standard, which provides a uniform set of guidelines acceptable to all health-related organizations in countries worldwide, whether transmitting to, or receiving personal health data from, other countries, should be complied with. (ISO 22857:2004 Health Informatics- Guidelines on data protection to facilitate trans-border flows of personal health information)

Principle 8: Personally identifiable health information should not be disclosed, except in circumstances authorised by law, court order or with the patient's specific, full and informed consent in writing.

Principle 8.1: Informed consent means that the patient or member should know the reasons why the disclosure is necessary (e.g. for the execution of duties in terms of a specific section of the Medical Schemes Act on, for example, waiting periods, and/or a specific regulation). The patient should also know and understand the implications such disclosure for him or her in

terms of health care delivery and -financing. Health care role players are encouraged to formulate the various purposes for which private information is required or should be disclosed, and whether such are authorised by legislation or whether specific *patient or member consent* is required.

Principle 8.2: The provisions of Section 8 of the National Health Act, Section 39 of the Child Care Act, Chapter 5 section 35 of the Mental Health Care Act, the Promotion of Access to Information Act and other relevant legislation relating to consent and participation in decisions affecting a user's personal health and treatment should be taken into account.

Principle 8.3: Where written patient authorisation is not possible Chapter 2 National Health Act, alternative generally acceptable means of identification may be used (e.g. "biometric consent"), subject to compliance with relevant legislation.

Principle 8.4: The same rules of confidentiality and consent to disclosure apply to dependants and steps have to be taken to ensure sufficient protection of dependant/ beneficiary confidentiality.

Principle 9: Where financial, ownership or shareholding links exist between a third party and a health care role player (such as a medical scheme, administrator, managed care organisation, intermediary or any health care role player), confidential- or personal information obtained by such role player in the course of its business as service provider, managed care organisation, medical scheme, administrator, broker may not be sold-, passed on to-, or be used by- or utilised in any manner by such third party institution or organisation for the purpose of conducting their business. The same prohibition applies where medical scheme benefits are linked to the conditions of work and/or employment contract. A contribution made by an employer towards an employee's medical scheme does not entitle that employer to access any personal- or health care information, including any medical diagnosis, held by the scheme or any health care role player.

Principle 10: Health care organisations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research purposes. The provisions of Sections 11, 15 and 16 of the National Health Act as well as internationally accepted research documents, such as the Helsinki Declaration have to be adhered to.

It is important to note that the legislation applies to all research, even where the researcher only uses existing files of patients and has no patient-contact at all.

Principle 11: Health care role players should not disclose personally identifiable health information to law enforcement officials or any other person acting in a capacity of investigating any alleged or suspected offence, in the absence of a compulsory legal process, such as a warrant or court order. Only relevant information may be supplied with regards to the purpose for which the information is to be disclosed, as stipulated within the framework of such warrant or court order.

Caution should also be exercised when information is requested by investigators acting on behalf of medical schemes. In such cases, written informed consent from the patient is a pre-requisite prior to any form of disclosure.

Principle 12: Health privacy protections should be implemented in such a way as to enhance and not undermine, existing laws prohibiting discrimination such as the Promotion of Equality and Prevention of Unfair Discrimination Act of 2000 and the Employment Equity Act of 1998. This principle also applies to issues such as profiling of practices and patient groups.

Principle 13: Strong and effective remedies for violations of privacy protections shall be established, including employee training and -disciplinary measures, appropriate contractual provisions and penalties with respect to any party contracting with a health care role player, etc.

Principle 14: All role players that handle healthcare information should be held accountable for breaches of privacy and confidentiality for information in their hold. Aggrieved persons should have access to internal procedures and/or outside institutions at which to lodge complaints.

The National Health Act creates penalties for health establishments and their staff in terms of violations of privacy/data protection, but similar penalties should exist for other role players in this sector.

REFERENCES

1. All Acts and other documents, as well as resource documents, referred to herein will be listed in an index to this document.
2. Constitution of the RSA Act 108 1996
3. The National Health Act 61 of 2003
4. Medical Schemes Act 131 of 1998 (as amended)
5. General regulations in terms of the Medical Schemes Act 131 of 1998 (as amended)
6. The Promotion of Access to Information Act. No 2 of 2000
7. SA Law Commission Issue Paper on Privacy and Data-protection
8. Electronic Communications and Transactions Act of 2002
9. ISO International Standard
10. Child Care Act 74 of 1983
11. Children's Bill
12. Insurance Act No. 27 of 1943
13. The Post Office Act No. 13 of 1974
14. Mental Health Care Act No 18 of 1973
15. Promotion of Equality and Prevention of Unfair Discrimination Act 52 Of 2002
16. Employment Equity Act 55 of 1998
17. Choice of Termination of Pregnancy Act No 92 of 1996 (as amended)
18. The Age of Majority Act No. 57 Of 1972
19. Ethical Rules of the HPCSA – Version June 2002
20. Criminal Procedures Act No. 51 of 1977
21. ICD 10 and the Right to Privacy and Confidentiality – Published by the Council for Medical Schemes – August 2003
22. Understanding Privacy and Confidentiality and the Promotion of Access to Information Act – Article by Adv. Kurt Worrall-Clare, April 2004
23. HPCSA Booklet 5: Making Professional Services Known
24. HPCSA Booklet 8: Guidelines for the management of patients with HIV infection or AIDS HPCSA
25. HPCSA Booklet 11: Guidelines on keeping of patient records HPCSA
26. HPCSA Booklet 13: National Patients' Rights Charter HPCSA
27. HPCSA Booklet 14: Confidentiality: Protecting and providing information HPCSA
28. HPCSA Booklet 15: Seeking patients' consent: The ethical considerations HPCSA