

Protecting healthcare information



By [Neil Kirby](#)

4 Sep 2014

There is rising concern as to the safeguarding of healthcare information, following the hacking of medical data of 4.5 million healthcare patients in the US, made possible by the Heartbleed bug.

Healthcare information, as a category of personal information, is the most sensitive information, as it carries the potential to cause a person embarrassment, expose them to ridicule or even social stigma.

Handing over one's personal information to a trusted healthcare provider is a daily activity for millions of people around the world, including South Africa. The laws concerning data protection and the manner in which personal information is handled vary from jurisdiction to jurisdiction.

Protection by the Information Act

In South Africa, the introduction of the Protection of Personal Information Act No. 4 of 2013 (PPI) introduces a new regime for the protection of personal information, particularly healthcare information. Whilst we are awaiting a date for the coming into effect of the Act, by proclamation by the President, measures are being effected in order to ensure that healthcare providers are able to comply with the rigors of the Act in so far as protecting personal healthcare information is concerned.

The Health Professions Council of South Africa (HPCSA), pursuant to powers under the Health Professions Act No. 56 of 1974, as amended (HPA), has set out principles that should be followed by healthcare providers, registered in terms of the HPA, when dealing with a patient's personal information and how to protect that information once it is in the possession of the healthcare provider.

However, the Council's rules do not bind every member of the healthcare sector as far as the rules apply only to those persons registered in terms of the HPA such as general practitioners, dentists and psychologists. This leaves an entire area of the healthcare sector without any particular rules including allied health practitioners, African traditional practitioners and health establishments ranging from clinics and hospitals to service providers assisting with the storage of stem cells and sperm banks.

Special personal information

The PPI identifies certain special personal information. As part of the category of 'special personal information' are the sub-categories of a data subject's health, sex life or biometric information. Accordingly, a great deal of attention is paid by the Act to the manner in which information concerning a person's health, sex life or biometric information (collectively

referred to as 'health information') is processed. Bearing in mind that the term 'processing' is defined as broadly as possible in the Act, any handling of information concerning health information by any other person will fall within the provisions of the Act. Fundamentally, a data subject or patient must consent to any processing of his or her health information or the processing must fall into one of the exclusion categories in the Act.

Processing information

Much attention is paid to the processing of health information in the Act. Whilst the Act does endeavour to allow for the processing of health information by medical professionals, healthcare institutions or facilities or social services, a number of conditions must be met in order for that processing to occur lawfully. Firstly, the processing must be necessary "for the proper treatment and care of the data subject" or secondly, for the administration of the institution or the provision of a professional practice, thirdly, the information must be subject to an obligation of confidentiality by virtue of "office, profession or legal provision."

A separate section of the Information Act is dedicated to the processing of information concerning "inherited characteristics." An outright prohibition exists in respect of the processing of such information, unless there is a serious medical interest that prevails or the processing is necessary "for historical, statistical or research activities."

Keeping information secure

That being said, while there may be relaxed rules in the Act concerning the processing of health information, it does not alleviate the obligation on persons processing such information to keep health information secure or to advise patients when compromises of their health information have occurred due to events such as hacking or any negligent exposure of the information to third parties. In this regard, the Act is careful in imposing security safeguards that must be adopted by all processes of information in order to ensure that personal information is not lost, damaged, destroyed without authorisation, susceptible to unlawful access or processing.

Therefore, the Information Act imposes particular obligations on people processing information to implement measures to:

- a. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- b. establish and maintain appropriate safeguards against the risks identified;
- c. regularly verify that the safeguards are effectively implemented; and
- d. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Written contracts needed

In addition, the Act requires particular steps to be taken to ensure that information is secure including written contracts between the healthcare practitioner and an operator, being the party who processes information for the healthcare practitioner or on behalf of the healthcare practitioner and requirements that healthcare practitioners must notify patients where information is compromised or unlawfully released. Such notifications must either be sent directly to the patient or published in the news media or prominently on the website of the healthcare practitioner. The Information Act prescribes the content of a notice of a security compromise as follows:

- a. a description of the possible consequences of the security compromise;
- b. a description of the measures that the responsible party intends to take or has taken to address the security compromise;
- c. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

- d. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

Confidentiality is paramount

In the context of health information, the possible consequences of health information leaking into the public domain are sometimes extremely severe for a patient. One must assess carefully how to describe to a patient the consequences of his or her information leaking into the public domain. The potential exposure for the healthcare practitioner of the consequences suffered by a patient are severe especially in so far as our courts have previously handed out damages for healthcare providers compromising patients' confidentiality in respect of a patient's HIV status.

Whilst the Act deals generally with information and its processing and control in South Africa, the processing of health information requires particular attention simply because of its sensitive nature and the consequences for patients if the information falls into the wrong hands. Just understanding how one would feel if one's health information did fall into the wrong hands or became publically available, one understands the need for the rigorous obligations to be fulfilled by healthcare providers in order to ensure that they are able to meet the requirements of the Information Act.

Hopefully, once the Act becomes law in South Africa, healthcare information will be properly and lawfully protected and data subjects will have lawful remedies where information is hacked, even by sophisticated bugs such as Heartbleed.

ABOUT NEIL KIRBY

Neil Kirby is director: health care and life sciences law of Werksmans. He is the chair of the Medicine and Law Committee of the International Bar Association. Kirby has been named as a leading lawyer in Dispute Resolution by Chambers Global: The World's Leading Lawyers for Business (2008 - 2013), and has published numerous articles in his various fields of speciality.

■ Protecting healthcare information - 4 Sep 2014

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>