Health Market Inquiry

Promoting Healthy Competition

competitioncommission south africa

Information Security Measures

Outline of the main precautions taken by the Inquiry to protect information against unauthorised disclosure

1 June 2015

Physical Security and Confidentiality

- The premises of the Health Market Inquiry ("the Inquiry") are access-controlled, with security personnel present 24 hours a day at the Inquiry offices.
- In addition, parts of the premises are electronically access-controlled in order to ensure that only duly authorised Inquiry personnel and Panel members have access.
- The Inquiry also has evidence rooms where hardcopy original documentation and information is stored. These evidence rooms are electronically access-controlled, with access limited to only two members of the Inquiry personnel. These rooms are also monitored 24 hours a day by CCTV cameras.
- The use of hardcopy documentation is strictly controlled and monitored. Checks are in place to ensure that information security procedures are observed by all members of the Inquiry team.
- All hardcopy documents have been electronically scanned into the Inquiry's Internal ICT System (see below). Team members are not permitted to work with the original hardcopies.
- Documents containing confidential information may not be removed from the Inquiry premises.
- All persons having access to confidential information (including, where relevant, consultants assisting the Inquiry) are required first to sign a confidentiality undertaking strictly prohibiting further disclosure and improper use of the information.

The Inquiry's Internal ICT System

- The Inquiry has a stand-alone ICT system that is separate from the general ICT system operated by the Competition Commission. There is no direct access or link between the two ICT systems.
- The Inquiry's ICT system includes a secure network that is access-controlled and limited to usage only by authorised members of the Inquiry team and the Panel. Consultants do not have direct access to the secure network. Where necessary, very limited access may be granted to a consultant for a specific assignment. In such instance the consultant will not be able to access information outside of the restricted access granted by the Inquiry.
- The system has purpose-built authorisation levels with full audit trail capabilities, which ensure that accessing, copying and printing of documents and/or information by any Inquiry member can be controlled, traced and reviewed.
- All access to and usage of the secure network is closely monitored by the Inquiry's Head of IT under the supervision of the Inquiry Director.

Data Management & Warehousing

- The Inquiry is in the course of receiving for processing a large amount of raw data from certain healthcare service providers. The Inquiry has secured the services of a specialist data warehousing and analysis service provider of global repute, for purposes of handling and processing this data.
- As explained in the Inquiry's bulletin on "De-Identification of Personal Data" (dated 1 June 2015), this data will as far as possible have been thoroughly de-identified so as to eliminate or otherwise limit the storage and processing of personal information.
- All such data obtained from stakeholders will be managed by the external service provider and will be warehoused and hosted off site from the Inquiry.
- In securing client data against improper use and unauthorised disclosure, the external service provider subscribes to international best practice, norms and standards.
- If further access to that data is needed by Inquiry personnel and Panel members, such access will be strictly controlled in conjunction with the precautions maintained by the external service provider.