Dr Margot Kerley
Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Dr Kerley

INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Please find attached the Department of Health and Ageing's written submission to your inquiry into the management and integrity of electronic information in the Commonwealth.

You will note that the submission is in two parts. The first contextualises my Department's position within the health information sector and the second specifically addresses the Terms of Reference. As you will note in the submission, the Department is taking a leadership role and making a significant contribution to further developing and improving a national framework through which electronic information throughout the health sector can be more effectively and securely managed.

Yours sincerely

(authorised for electronic transmission)

Jane Halton
Secretary

17 December 2002

Commonwealth Department of Health and Ageing
Submission to
JCPAA INQUIRY INTO THE INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Overview

Background to submission

This submission is in response to the invitation extended by the Joint Committee on Public Accounts and Audit regarding its inquiry into the management and integrity of electronic information in the Commonwealth.

Health Portfolio Information Management Context

The health portfolio's information environment is highly complex, both in structure and in the variety and quality of the information it gathers. Accurate, high quality information is critical to the success of all aspects of the Australian Health Care system as it assists in developing and managing system improvements and efficiencies. Improving the quality of health care requires commitment, leadership, resources and sustained effort at all levels of the health care system. The ongoing challenge is to develop national mechanisms which will optimise use of data already collected, and enhance information quality and integration between data sources without compromising information confidentiality, privacy or security.

Australian Health Information Governance

The Australian health system has a diversity of arrangements for planning, funding, delivering and regulating health services which feature a mix of private and public sector involvement. However, the health system is primarily financed and governed by the two tiers of government, represented by the Commonwealth Department of Health and Ageing and the State and Territory health authorities.

Together with the Health Insurance Commission (HIC), the Australian Institute of Health and Welfare (AIHW) and the Australian Bureau of Statistics (ABS), these government agencies play leading roles in the collection and reporting of information on health and wellbeing. Under the National Health Information Agreement 1993 (NHIA), to which these agencies are signatories, the National Health Information Development Plan (NHIDP) sets out agreed national priorities for health information to be considered by the Australian Health Ministers' Advisory Council (AHMAC). The National Health Information Management Group (NHIMG) was established to oversee the implementation of NHIA.

In July 1998 Australian Health Ministers established the National Health Information Management Advisory Council (NHIMAC) as the peak body for progressing key issues regarding the use of information in the health sector. The Council's role is to:

- advise Health Ministers on options to promote a nationally uniform approach to more effective information management within the health sector;
- promote the efficient and effective use of information technology in health;
- develop a partnership with the private health and information technology sectors;

- encourage the development of a market for Australian health information technology and services; and
- protect the public interest – particularly in relation to privacy.

Since its establishment, the council has guided the development of both the first and second editions of *Health Online:* A *Health Information Action Plan for Australia*, in collaboration with Commonwealth, state and territory governments. The action plan provides stakeholders with a national position on directions for health information standards in the health sector and the basis for further investment of effort and resources.

Health Online: A *Health Information Action Plan for Australia* is a key strategic tool. It formalises the importance of national standards in achieving an integrated approach to health information management and information technology (IM/IT). The major benefit of the Plan is that it presents a clear statement for key stakeholders on:
- the direction national standards development should take;
- what national standards should be developed, including those standards that need to be congruent with international standards activity;
- who should be responsible for the development of national standards; and
- how the development of national standards should be funded.

With this in mind, links between the specialist groups within the health sector have been strengthened and formalised through the establishment and membership of the National Health Information Standards Advisory Committee (NHISAC) under the auspice of NHIMAC.

NHISAC has opened the way to ensure policy work combines with national standards development and implementation activities to avoid duplication and wasted effort. It does so within a context that recognises the need to systematically progress the health information agenda in a cooperative and coordinated way as a joint industry and Commonwealth-State priority, and in a manner that still allows industry innovation.

Health Information Infrastructure

Australia has established, through processes such as the NHIA, an infrastructure which supports the collection and dissemination of comparable data and, hence, assists in providing a cost-effective information system. Some fundamental elements of this infrastructure are:
- frameworks, such as the National Health Performance Framework, to provide conceptual and operational structure to the collection and reporting of data on health activities;
- National Minimum Data Sets (NMDS) in areas where State and Territory administrative data are integrated for national reporting;
- national standards and definitions incorporated into the National Health Data Dictionary; and
- adoption of internationally endorsed health classifications, with nationally endorsed Australian modifications where necessary.

National Health Performance Framework

One key framework which guides collection and reporting of data on health activities in Australia is the National Health Performance Framework (NHPF). In 1999 Australian Health Ministers set up the National Health Performance Committee, to report on the national health system encompassing the acute, community health care and public health sectors. Through a wide consultation process, the Committee has developed the framework and appropriate indicators as a basis for its reporting.

The Australian framework has three basic tiers of information:

- health status and outcomes;
- determinants of health; and
- health system performance.

This three-tier framework allows monitoring on how health system interventions can focus on managing determinants, as in public health programs, as well as those that directly relate to the treatment of diseases.

National Health Data Dictionary and Knowledgebase.

Under the NHIA, the National Health Data Dictionary (NHDD) is the authoritative source of health data definitions used in Australia where national consistency is required. It was first published in 1989 and is produced each year by the National Health Data Committee, a standing committee of NHIMG. It is accompanied by the web-based Knowledgebase which is Australia's health, community services and housing metadata registry. The scope of the Knowledgebase continues to expand, providing standard definitions for administrative data collections, population health collections, and recent activities have established the NHDD as the repository for terms required for future electronic health records.

National Minimum Data Sets

National Minimum Data Sets (NMDSs) have been established for mandatory collection by jurisdictions. NMDSs underpin national reporting from administrative data collections relating to health service encounters. To date, approximately twenty NMDSs have been established, for example Admitted Patient Care NMDS and Public Hospital Establishments NMDS. Jurisdictions are responsible for the supply of data for NMDSs and, in most cases, the AIHW compiles and disseminates national results.

Health Classifications

Where applicable, Australia uses international classifications such as ICD in administrative and population based health collections. The National Centres for Classification in Health (NCCH) with responsibility for morbidity classifications has developed ICD-10-AM (Australian Modification) for use in clinical settings. Revisions of ICD-10-AM are approved by NHIMG, which also has responsibility for health classifications used in NMDSs and, more broadly, in the NHDD. The National Electronic Health Records Taskforce recommended that an Expert Group on Classification and Coding be established by NHIMG, to guide development and adoption of classifications for electronic health records.

National Legislation

Federally, the privacy, confidentiality and security of information is protected through legislation such as the Privacy Act 1988, Telecommunications Act 1997, Freedom of Information Act 1982, Health Insurance Act 1973, and National Health Act 1953. Mandated standards at the national or State/Territory level, such as the Data-Matching Program (Assistance and Tax) Act 1990, provide additional guidance and assist in facilitating more consistent information.

National Health Privacy Code

Privacy is a fundamental principle underpinning quality health care. It is important that a strong and effective health specific privacy framework is in place to regulate how and when an individual's personal health information may be collected, stored and disclosed to others. Currently there is little consistency across the Commonwealth, States/Territories, and private sector. For example, personal health information held in the private sector is protected under the Privacy Amendment (Private Sector) Amendment 2000. NSW, Victoria and the ACT also have health specific privacy legislation in place. The Northern Territory is developing health specific legislation. South Australia and Queensland have administrative regimes in place. The result of these different approaches is the emergence of the 'rail guage' problem, where different standards apply in different states.

To overcome these difficulties, the National Health Privacy Working Group - a sub group of AHMAC - was established to develop a health specific privacy framework. The key to this framework is the National Health Privacy Code.

The aims of the Code are to:

- Safeguard the health privacy and dignity of all individuals;
- Achieve national consistency in health privacy protection across jurisdictions and between the public and private sectors; and
- Take into account changes in the way personal health information is handled as a result of technological change.

Department of Health and Ageing's Internal Environment

The Department is committed to ensuring the security, privacy and confidentiality of the data it receives and this is reflected in its arrangements with information providers and internal processes which have been developed. DoHA also has a strong commitment to improving the management and flow of information between agencies in order to achieve its outcomes.

The Department has a leadership role in improving health outcomes across the health sector. Within this role, the Department requires quality information for the purposes of policy development, evaluation and payments. Through this information, the Department actively contributes to improving health outcomes. This contribution is both direct, such as the delivery of services, and indirect, such as its involvement in the national health information governance framework. This framework is responsible for providing national processes to ensure accuracy, security and integrity of information. The Department has ensured that its internal processes complements and augments these national processes.

The main personal level health data sets made available to the Department are the Medical Benefit Scheme (MBS) and Pharmaceutical Benefits Scheme (PBS), provided by the Health Insurance Commission (HIC); and hospital morbidity data, provided by the States and Territories. DoHA receives this information in a de-identified format and uses it for specific purposes as set out in Commonwealth legislation and inter-agency agreements. Ownership of this data is retained by the providing agencies, whom also ensure data integrity. Privacy, confidentiality and security issues are addressed by providing agencies through relevant legislative and governance processes. Once within the Department, access to this information is strictly controlled.

Additionally a variety of data is collected by the Ageing and Aged Care Division of the Department. This Division has established a number of information systems and electronic data repositories to enable it to fulfil its functions of providing policy advice, managing programs and payment of subsidies. This information ranges from individual data (both identified and de-identified) to service providers, services, and demographic data. Cooperation with the Department of Veteran's Affairs, Centrelink, the Department of Family and Community Services and the HIC facilitates coordinated service delivery and payments accountability. National legislation, external and internal security controls ensures the privacy, confidentiality, and security of this information.

The Department also holds a large quantity of program, or administrative, information. This includes data from other administrative payment systems such as Indigenous health, grant payments to research organisations, and funding to ongoing programs such as the National Health Priority Areas all of which are administered through the Department. The systems that capture this data were primarily designed for payments purposes and are suitable predominantly for payments processing but not for further analytical purposes. This information contains specific organisational-level detail, but little at the individual level. Such information is usually "x-in-confidence" material and is handled, stored and accessed in accordance with legislative and Departmental procedures.

Other information is obtained via agreements with other Commonwealth agencies, non-government organisations and research bodies. They include ongoing and one-off survey data, data linkage projects, and pilot projects. Like the MBS, PBS and hospital information, this information is provided in de-identified form, for particular purposes, and in accordance with relevant legislative and governance frameworks. Once this information is held by the Department, it is stored and handled in accordance with national and Departmental processes.

Departmental Legislation, Chief Executive Instructions and Procedural Rules

The core elements of the electronic health information management governance and legislative framework are described above. Specific Commonwealth legislation to which DoHA is required to comply is listed at Attachment A.

Through its governance and organisational structure, DoHA fosters a culture in which soundly managing and improving the quality and use of information while ensuring privacy and security needs are met is paramount. Internally, the Chief Executive Instructions, Procedural Rules and other internal directives provide guidance on information management aspects such as security, privacy, legislative compliance, risk management, audit and confidentiality. Training and development opportunities in these areas are also available to all staff.

Departmental Governance Structure

The Information Planning and Privacy Committee (IPPC) has provided the primary internal information management and privacy governance mechanism. It is responsible for considering and progressing existing and emerging information and privacy issues and monitoring developments under the Department's Information Management Plan 2001-2003 (IMP).

The IMP outlines the key strategic goals for the Department's information management and plans for meeting them. IPPC's annual work program is based on strategic issues of particular importance from this plan.

To ensure that the Department's priorities and goals are better aligned with the Government's policy directions, Departmental governance arrangements are being revised and improved. This has included the establishment of Chief Information Officer (CIO) and Chief Operations Officer positions. It has also resulted a re-evaluation of the Departmental Committee structure. The resulting evolution is consistent with the ANAO's Better Practice Guide, A*pplying Principles and Practice of Corporate Governance in Budget Funded Agencies*.

The revised Departmental arrangements will better reflect the increased importance for effective leadership on, management and integration of information issues within the public sector. To this end, a new Information and Communication Division is being established which will be headed by the CIO. Under this Division there will be a more cohesive and consistent approach to internal and external information management, privacy and communication issues. It is anticipated that this structural realignment will prove a key step in the Department's provision of ever-improving, responsive, and appropriate health policy, program development and service delivery.

Departmental Electronic Service Provision

In accordance with the *GovOnline* strategy, the Department has moved to complement its traditional service delivery through developing and tailoring online services that are easy to use and allow people to easily interact with the Department. The *GovOnline* agenda provides an opportunity for many areas within the Department to extend their services to stakeholders previously difficult to reach, particularly in rural and remote areas. In a range of cases the online agenda will also allow new services to be offered.

Examples of the means by which electronic services are provided include:

- computer to computer style electronic business with various trading partners;
- Internet delivery of health information which is vetted by experts;
- lodgement and tracking of grants; and
- lodgement and tracking of applications for new drugs and devices.

HealthOnline

Potentially one of the most significant of these services will be *Health Online: A Health Information Action Plan for Australia* has been developed. It is Australia's proposed network of electronic health records that aims to improve the flow of information across the health sector. If developed in full, it will allow consumer health information to be collected electronically, safely stored and exchanged between authorised health care providers, within strict privacy safeguards.

Emerging Directions

Data Linkage

The ability to link hospital morbidity data with data generated by the MBS and PBS is essential to any thorough attempt at coordinating hospital, medical and pharmaceutical care, due to the Federal nature of constitutional responsibilities for health service delivery in Australia. Recently there have been an increasing number of policy issues where the absence of capacity to link national hospital data has had an adverse impact. Noting this, in early 2002 AHMAC requested that NHIMG consider how to best enable jurisdictional hospital morbidity unit record data to be linked to other unit record data for the purpose of enabling high priority research and analysis to improve health outcomes and health service delivery.

Over the last five years the Department has conducted several projects in collaboration with the States, utilising linked health care data. Data sets currently held include hospital, MBS and PBS data relating to residents of WA and QLD, with deaths data included from the National Death Index for diabetics in WA. The Department is cognisant that additional security measures are required when using data for record linkage. A 'best practice' approach has been developed by the Department and published in the scientific literature.

In general, legislative control of the various administrative data sets allows use of the data for purposes defined as 'necessary in the public interest'. Access to the various data sets is provided under and consistent with the:

- Information Privacy Principles contained in the Privacy Act 1988;
- Health Insurance Act 1973; and
- National Health Act 1953.

TOR 1. The Privacy, Confidentiality And Integrity of the Commonwealth's Electronic Data

The Department recognises that privacy and confidentiality of electronic data is important to the broader Australian community. Accurate and up-to-date health information is fundamental in aligning the strategic direction of the Department with community needs and in improving health outcomes for all Australians. The Department is aware of the potential consequences for the wider community if it does not ensure privacy, confidentiality and integrity of its electronic data. The consequences are further compounded by the sensitive health information that the Department deals in. To this end the Department is committed to protecting and ensuring the privacy, confidentiality and integrity of electronic data.

The Department is required to comply with the *Privacy Act (1988)*, the tax file number guidelines issued under section 17 of the *Privacy Act (1988*) and the *spent convictions scheme* as provided for by the Crimes Act. The Department is bound by the Medicare and Pharmaceutical Benefits Programs legislation and privacy guidelines and is also affected by privacy rules set out in other laws, including secrecy provisions in other legislation.

Specifically, the Department of Health and Ageing is required to comply with the Information Privacy Principles (IPP), and under IPP 5.3 in s.14 of the *Privacy Act 1988* must maintain a personal information digest (PID). The PID details the personal information held by the Department and outlines:

- the nature of the various types of records of personal information kept by the Department;
- the purpose for which the records are kept;
- the class of individuals to which the records apply;
- the period for which the records are kept; and
- details of how individuals can get access to records about themselves.

In line with the Privacy Commissioner's requirements, the Digest is submitted and published annually, and it is available internally. In 2002, the Department undertook a comprehensive exercise to ensure the completeness of its personal information digest.

The Information Planning and Privacy Committee (IPPC) is a strategic forum through which existing and emerging DoHA information and privacy issues are considered and progressed. The IPPC commissioned a review of the Department's compliance with legislative and other external requirements with respect to Privacy and the *Privacy Act 1998* as a component of its 2001-2002 work program.

An independent review of the Department's compliance with privacy requirements, including privacy principles and legislation, was completed in August 2002. The review found that the Department is "*essentially privacy compliant*". The report goes on to say "*There is a strong implicit culture of privacy protection; some of this flows from the secrecy and confidentiality provisions applying to DoHA*".

The report noted that while the Department has in place policies, procedures and administrative processes in order to ensure privacy compliance, some risk exists from the lack of whole-of-department consistent and systemic policies and administrative procedures. Specific systemic deficiencies identified included:

- ongoing privacy training and awareness across the Department;
- privacy exposures created by contracted external parties; and
- the absence of privacy procedures in some areas.

IPPC considered the Privacy Compliance Report in September 2002 and endorsed an action plan to address privacy risk issues identified by the consultant. The Department will have its complete system in place from early 2003 to ensure ongoing privacy compliance. Staff and resources within the Department have been allocated to the action plan, and the work program is under way.

Significant components of the action plan include:

- developing a Departmental privacy manual;
- developing an internal privacy officer network;
- reviewing and extending training and awareness programs;
- identifying key risk areas and examining and refining relevant privacy policies and procedures;
- reviewing and refining Departmental privacy guidelines and procedures;
- reviewing contracting guidelines to ensure privacy compliance by contracted external parties; and
- establishing a process to continue to identify and evaluate emerging issues.

TOR 2. The Management and Security of Electronic Information Transmitted by Commonwealth Agencies

The Department recognises the value of the electronic information that is transmitted both internally and externally and is cognisant of the associated importance of maintaining a high standard in managing and securing electronic information. It sets a very high value on information privacy and is aware of potential impacts that lapses in security may have on the broader community. The maintenance of the high standard of management and security of electronic information is a reflection of the culture of the organisation and the value set of its workers. The Department undertakes a leadership role and is committed to best practice for the management and security of transmitted electronic information.

To this end electronic information is actually managed with more rigour and safeguards than was ever applied in the days of purely paper based correspondence. A formal control framework is in place under Chief Executive Instructions which are in turn supported by a policy and procedural framework. These policies and procedures are enacted in terms of staff training, individual awareness and an automated set of safe guards to manage and secure electronic information.

Procedural safeguards include:

- regular audits of IT systems and infrastructure;
- trading partner agreements laying out the protocols for electronic commerce;
- a Security Policy area that assists clients in assessing the risk to their information holdings, develops the overall security policy and conducts risks assessments;
- designated "owners" of individual data holdings who are responsible for applying proper safeguards to information holdings in line with policy; and
- appropriate business continuity plans that address systems, e-mail, browser services and Web sites.

Automated safe guards include:

- hardware secured networks between trading partners such as the HIC;
- system Security Plans for each system, including those that communicate externally to the Department; and
- e-mail encryption (currently being trialed).

Data Storage and Access

The Department's infrastructure and some services are leased from IBM GSA. IBM GSA are contractually obliged to protect the information holdings of the data to the same extent that applies to Departmental staff. Automated safeguards are also in place to protect the Department's information holdings, including audit logs of all access and security software to enforce separation of duties and restrict access to that required for service delivery.

IBM GSA staff have appeared for the Government in testifying to the IT security framework in legal cases.

The Department's Internet Publishing Standards and Change Control Procedures ensure that all information published on the Internet complies with the Government Online Strategy and the Electronic Transactions Act 1999.

ANAO Audit - Information Technology at the Department of Health and Ageing

In July 2002 the Auditor-General released a report to the Parliament detailing the results of an audit into information technology at the Department. The report found that:

(i) at the operational level, applications systems reviewed are delivering the required business outputs in an effective and controlled manner;
(ii) the management and operation of IT taken as a whole demonstrated compliance with better practice;
(iii) the applications reviewed during the audit can be relied upon to achieve effective results;
(iv) extensive testing found the data to be accurate, complete and consistent; and
(v) Health had implemented an appropriate level of management reporting to monitor the accuracy, completeness, consistency and currency of data.

Transmission of Information

Information transferred to and from the Department typically takes place in 3 different fashions:

- over hardware encrypted lines to fellow Government agencies;
- over software encrypted sessions to Departmental systems;
- via unencrypted e-mails.

The Department is aware of the vulnerability of unencrypted e-mail transmission over the Internet and staff are made aware of proper e-mail procedures. Work is underway in developing encrypted e-mail solutions, however this is a complex and costly solution and will take some time to implement.

TOR 3. The Management and Security of the Commonwealth's Electronic Information Stored on Centralised Computer Architecture and in Distributed Networks

The Department is cognisant of the importance of maintaining a high standard when managing and securing electronic information stored on centralised computer architecture and in distributed networks. It, as with all Commonwealth departments and agencies, is required to comply with the Protective Security Manual (PSM) issued by the Protective Security Coordination Centre within the Attorney-General's Department. The PSM requires Information Systems Security Policy and the implementation of plans to ensure systems are appropriately protected.

Electronic information stored on the Department's IT architecture in both central and remote locations and transmitted across its network is covered by a wide range of safeguards.

Additional procedural controls include:

- system control frameworks for appropriate systems that address issues such as separation of duties, recording of key transactions and audit logs;
- a comprehensive data backup regime from individual transactions to full warehouses with backups being stored external to the Department; and
- industrial strength security packages protecting all appropriate systems, which are capable of protecting systems in a wide range of mechanisms from simple logon/password down to protecting individual items of data being displayed.

Applications Development

All applications developed by and for the Department are required to comply with Chief Executive Instructions 1.8, Ensuring Integrity of Computer Systems, and 1.9, Information Technology and Telecommunications Security.

Adequacy of IT Processes

IT processes within the Department are regularly audited and a process for continuous improvement is in place under the standard Government process for control of IT (CobIT - Control Objectives for Information and related Technology) and the Capability Maturity Model.

TOR 4. The Adequacy of the Current Legislative and Guidance Framework

Current legislation and guidelines provide a sound framework for the management of electronic information in the portfolio. A number of the Acts administered by the Department contain secrecy provisions for the handling of personal information, such as the *National Health Act 1983*, the *Aged Care Act 1997* and the *Disability Services Act 1986*. The secrecy provisions regulate how the Department uses and discloses private and confidential information. Some of the Acts also contain penalties for breaches of these provisions.

Additionally, the Department is bound by a number of other Commonwealth Acts and guidelines that govern the management of information, such as the *Privacy Act 1988*, the *Archives Act 1983*, the *Financial Management and Accountability Act 1997* and the *Commonwealth Protective Security Manual 2000*. A list of applicable legislation and guidelines is at Attachment A.

The *National Health Privacy Code* provides additional guidance on the management of electronic health information.

Whilst it is important for the Department to maintain a high level of privacy and confidentiality in the management of information relating to individuals, the current legislative framework does, at times, restrict the Department in delivering its business through an electronic environment. Issues can arise in the implementation of some Government services where there is specific legislation detailing the instruments and procedures required of consumers accessing these services; for example, the legislation may reference a specific paper based form, which can constrain the delivery of electronic services.

Also, the legislation was not written to support the use of health administration data for health service monitoring, quality assessment or surveillance. Restrictions on the use of these data basically limit their use to the management of payments. Recent interest in the uniqueness of these data and the need for information otherwise unavailable has resulted in some linkage and analysis being conducted. However, a more streamlined approval process for Departmental use of these data is needed to fully capitalise on this resource.

Attachment A:

Legislation Applicable to DoHA

REF	LEGISLATION
	Administrative Decisions (Judicial Review) Act 1977
112 of 1997	**Aged Care Act 1997**
	-related and consequential Acts
114 of 1997	**Aged or Disabled Persons Care Act 1954**
	Archives Act
	Agricultural and Veterinary Chemicals Act
12 of 1914	**Crimes Act 1914**
6 of 1901	**Customs Act 1901**
138 of 2002	-Customs Regulations 1926
335 of 2001	-Customs Amendment Regulations 2001
212 of 2000	-Customs (Prohibited Exports) Amendment Regulations 2000
213 of 2000	-Customs (Prohibited Imports) Amendment Regulations 2000
	Data-Matching Program (Assistance and Tax) Act 1990
129 of 1986	**Disability Services Act 1986**
162 of 1999	**Electronic Transactions Act 1999**
137 of 2001	-Electronic Transactions Amendment Regulations 2001
154 of 1997	**Financial Management and Accountability Act 1997**
3 of 1982	**Freedom of Information Act 1982**
	Gene Technology Act
132 of 1995	**Health and Other Services (Compensation) Act 1995**
42 of 1974	**Health Insurance Act 1973**
81 of 1997	**Hearing Services Administration Act 1997**
184 of 1985	**Home and Community Care Act 1985**
	Industrial Chemicals Notification and Assessment Act
95 of 1953	**National Health Act 1953**
119 of 1988	**Privacy Act 1988**
	- Federal Privacy Amendment (Private Sector) Act 2000
147 of 1999	**Public Service Act 1999**
47 of 1997	**Telecommunications Act 1997**
21 of 1990	**Therapeutic Goods Act 1989**
	-Therapeutic Goods Amendment Regulations 2000
27 of 1986	**Veterans' Entitlements Act 1986**
46 of 1991	**Social Security Act 1991**
	Tax Acts

Best Practice

- "*Better Practice Guide – Internet Delivery Decisions"* (ANAO May 2001).
- *"Guide to Minimum Website Standards"* (NOIE, March 2001)
- "*Record Keeping Metadata Standard for Commonwealth Agencies*" (National Archives, 1999)
- *"Guidelines for Keeping Records of Web Based Activity in the Commonwealth Government"* (National Archives, March 2001)
- *"DIRKS – A Strategic Approach to Managing Business Information"* (National Archives, March 2000)
- *Office of the Federal Privacy Commissioner – consultation paper on "Privacy Issues in the use of public key infrastructure for individuals and possible guidelines for handling privacy issues in the use of PKI for individuals by Commonwealth Agencies"*, June 2001.