Health information systems in Australia are undergoing rapid change. In common with other western countries, the growing importance of population health data and health outcomes research to future improvements in health status, has precipitated vigorous debate in Australia about the legal regulation of health data flows and the reasonable limits of privacy. In this paper, I will review the regulation of personal health information in health research, focusing on data linkage, and the regulation of health databases. I will assess trends in the regulatory environment, including the challenges posed by ‘on-line’ health information networks. A feature of research claims to patient data is the potential for the data to benefit public health, although not necessarily the immediate patient. As Schultz notes, epidemiological research raises two themes that are now well established in the laws and bioethics standards of western countries. The first is the issue of consent to involvement in research, a requirement that secures individual autonomy and freedom, and winds back the power imbalance between patients and their doctors (an imbalance exacerbated by the bureaucratisation of medicine and the rapid development of medical technology). The second theme is the risks to privacy posed by modern health information systems, a factor exacerbated by the emergence of on-line networks. Together, consent and...
privacy protect individual dignity and autonomy, and should be regarded as public health values in addition to being individual interests.3

Research claims are distinct from, although they may overlap with, both managerial claims to health data, and commercial claims. Managerial claims include the use of patient data for billing, funding and verification of service, service-monitoring, complaint-handling and accreditation, quality assurance and clinical audit, and medico-legal purposes. Commercial claims include the use of health data for market surveillance, product development (for example, clinical trials), and direct marketing. In general, the use of personal health information for managerial purposes is less contentious (and less regulated) than the use of data for research purposes.4 On the other hand, the recently enacted private sector privacy legislation does not permit the disclosure or use of personal health information for direct marketing at all, without the patient’s prior consent.5 Hitherto, there have been numerous reports of drug companies obtaining access to patient identities.6

There are four 'layers' of regulation relevant to determining the circumstances in which it is lawful to collect, store and disclose identifying, or identifiable (coded, but re-identifiable) data for research purposes. Firstly, there are issues relating to the existence and limits of duties of confidentiality owed under equitable or contractual principles. Secondly, confidentiality has a statutory

3 On a number of occasions, courts have recognised that the effective functioning of the health care system depends on public trust, secured through the protection of privacy and confidentiality: Duncan v Medical Disciplinary Committee [1986] 1 NZLR 513 at 521; X v Y [1988] 2 All ER 648 at 653; Jaffee v Redmond 116 S Ct 1923 (1996) at 1928. As Mandl et al note: 'If patients feel that they have no control over the fate of their medical information, they might fail to disclose important medical data or even avoid seeking medical care because of concern over denial of insurance, loss of employment or housing, or stigmatisation and embarrassment. Expectation of privacy allows trust and improves communications between doctors and patients': Kenneth D Mandl, Peter Szolovits & Isaac S Kohane, 'Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private' (2001) 322 British Medical Journal (on-line) 283–287.

4 The federal Privacy Commissioner's private health sector guidelines, issued under the Privacy Act 1988 (Cth) s27(1)(e), permit personal health information to be used and disclosed for the 'managerial' purposes noted above 'where the use or disclosure of de-identified data will not suffice, and provided it is within the reasonable expectations of the individual': Office of the Federal Privacy Commissioner, Guidelines on Privacy in the Private Health Sector (October 2001) 14–15.

5 Id at 17; compare Privacy Act 1988 (Cth), Schedule 3, National Privacy Principle 2.1(c).

6 For example, 'GP Warns on Privacy Breach' Australian Doctor (27 April 2001) at 2; 'Drug Reps to Lose Access to Records' Australian Doctor (20 July 2001) at 11; 'Pfizer Denies GP's Privacy Allegations'. Australian Doctor (3 August 2001) at 4. See also 'Doctors Worried About Ethics of Patient Database' Sydney Morning Herald (30 December 2000) at 2; 'Privacy Worry Puts GP Research at Risk' Australian Doctor (16 March 2001) at 3. Tim Dixon, director of the Australian Privacy Foundation, cites a case where a woman was approached by a health services company trying to sell her a treatment package after the woman had undergone a diagnostic test a few days previously. In Canada, a woman diagnosed with terminal cancer was offered a 'special package deal' by a funeral company: 'Health, Privacy and the New Technology'. The Law Report, ABC Radio (27 February 2001) <http://www.abc.net.au/rn/talks/8.30/lawrpt/stories/6251767.htm>.
dimension, since most jurisdictions have non-disclosure provisions in health services statutes, and public health statutes. Most but not all of these provisions apply to public sector-held health information.\(^7\) In addition, there are a variety of HIV specific provisions.\(^8\) Thirdly, legislatures are progressively enacting privacy legislation. Information Privacy Principles having statutory force currently apply to Commonwealth agencies,\(^9\) to public sector agencies in NSW,\(^10\) to both the public and private sectors in Victoria and the ACT,\(^11\) and since 21 December 2001, to the private sector.\(^12\) A trend towards health-specific privacy legislation is also evident. Health privacy statutes exist in Victoria and the ACT, with a Bill before the NSW Cabinet at the time of writing.

A feature of statutory privacy principles is that they distinguish between the ‘primary’ purpose(s) for which the information was collected or generated (for example, clinical care), and other ‘secondary’ purposes for which it could potentially be used (for example, research). In the absence of consent, privacy legislation constrains the use and disclosure of information for secondary purposes, subject to narrowly defined exceptions. Further layers of privacy protection applicable to on-line health information systems seem destined to arise as current proposals for HealthConnect, the Better Medication Management System (BMMS), and other health information networks take shape.\(^13\) Finally, from an ethics perspective, there is the question of compliance with the National

---

7 For example, *Health Administration Act* 1982 (NSW) s22; *Public Health Act* 1991 (NSW) s75; *Mental Health Act* 1990 (NSW) s289; *Health Services Act* 1988 (Vic) s141 (also applies to private hospitals); *Mental Health Act* 1986 (Vic) s120A; *Health Services Act* 1991 (Qld) s63; *Health Act* 1937 (Qld) ss100E, 100FO, 1001; *Public and Environmental Health Act* 1987 (SA) s42; *South Australian Health Commission Act* 1976 (SA) s64.


9 *Privacy Act* 1988 (Cth) s14.

10 *Privacy and Personal Information Protection Act* 1998 (NSW).

11 *Health Records (Privacy and Access) Act* 1997 (ACT); *Health Records Act* 2001 (Vic); *Information Privacy Act* 2000 (Vic).


Statement on Ethical Conduct in Research Involving Humans. The impact of the ‘layers’ of regulation noted above is uneven across both jurisdictions and sectors. The extent to which physicians, health care organisations, researchers and database administrators currently comply with laws relating to confidentiality, privacy and consent, and with the National Statement, is unknown.

The regulation of research claims to health data is a pressing issue that will become increasingly important in future. On the one hand, the trend in health privacy protection is towards an increasingly complex, and constraining, web of legislation. This creates logistical and compliance problems for researchers, and others contributing to the development of health data assets (including database administrators, and physicians reporting data). On the other hand, future improvements in public health will increasingly depend on the more effective use of health data resources: in order to monitor trends in health status, to investigate the causal roles of ‘lifestyle’, environmental and other risk factors within the degenerative diseases that increasingly account for morbidity and mortality, to measure and improve the quality and performance of health care services, and to develop ‘best practice’ for prevention and care. Epidemiologists and population health researchers, in particular, are keen to unlock the public health value of clinical data by — essentially — making clinical health information systems a subset of a broader public health information system that encompasses demographic, socio-economic and environmental data. The growth of health informatics, and the capabilities of on-line health information systems further highlight the potential for an overlap between clinical care, health research and public health

---

14 National Health and Medical Research Council (NHMRC), National Statement on Ethical Conduct in Research Involving Humans, June 1999: <http://www.health.gov.au/nhmrc/ethics/statement.htm> (hereafter ‘National Statement’). The National Statement is a series of ethics guidelines developed by the Australian Health Ethics Committee (AHEC), a principal committee of the NHMRC, and issued by the NHMRC pursuant to its statutory obligations under the National Health and Medical Research Council Act 1992 (Cth) ss71(a)(iv)-(v), 8, 90–91. Under this Act, the NHMRC has a national role advising the Commonwealth Government, other Australian governments and the community on matters relating to public health, health care and medical research. Under the National Statement (Ch. 2), universities, hospitals and other research bodies are required to establish and to resource Human Research Ethics Committees (HRECs) to scrutinise and monitor research protocols, applying the ethical principles set out in the National Statement.

15 Dr Christopher Clarke, Past President, Thoracic Society of Australia & New Zealand (TSANZ) and the author recently completed a small pilot exploring the kinds of voluntary research registers that exist within thoracic medicine in Australia, and their compliance with privacy laws and the NHMRC Statement. From a sample of seven databases, only one had sought ethics approval, none had obtained patient consent, three received name-identifying data, and of the four receiving data reported under code, in all but one case the data could be re-identified. See also John W Donovan, ‘An Experiment in Privacy Protection’ (1984) 141 Medical Journal of Australia 648.

16 See further, Part 3.B below.

17 ‘Health informatics’ has been described as an evolving scientific discipline that deals with the collection, storage, retrieval, communication and optimal use of health related data, information and knowledge: Parliament of the Commonwealth of Australia, Health On Line: A Report on Health Information Management and Telemedicine (October 1997) 5.
functions. Similarly, the influence of ‘evidence-based medicine’ and the impact of resource constraints have given massive impetus to research evaluating the effectiveness of both public health programs and various forms of clinical care in terms of observable indicators, or ‘health outcomes’. Many of these studies necessarily build upon clinical data. In general terms, therefore, the tension between health research and health privacy is set to continue.

Part 1 of this paper sets the scene for discussion of these issues by providing some examples of the ‘data needs’ of particular research methodologies. It also reviews the role of health databases as sources of data in data linkage studies. Part 2 provides a detailed review of the current regulatory environment of health research. It illustrates the fragmentation and complexity of current laws, and suggests ways in which the law might be modified and rationalised to better facilitate research claims and to balance them with privacy interests. In view of the increasing importance of health research to future gains in health and wellbeing, a national approach to this area is required.

On balance, there is unrelenting and probably irresistible pressure for the development of ‘multi-function’ health records whose purpose goes beyond patient care to include epidemiological and clinical outcomes research, quality assurance and cost monitoring functions. As medical records move ‘on-line’, and the centralisation and coordination of health data becomes possible, the demands for third party access, the potential benefits of providing such access, as well as the privacy risks for individual patients, will all increase. Part 3 reviews recent progress towards integrated, electronic health care records in Australia, together with the privacy risks posed by these developments. Privacy advocates need to consider their priorities in this new environment and to be realistic about the parameters within which privacy controls will be fashioned. The paper concludes with a modest proposal for how a research specific, unique patient identifier might be integrated within an on-line environment in order to facilitate health research, while minimising loss of privacy. Overall, the paper advocates

---

18 See George I. Rubin & Michael S Frommer, ‘Evidence-Based Medicine — Time for a Reality Check’ (2001) 174 Medical Journal of Australia 214. Goodman notes that ‘research on outcomes, practice guidelines, and evidence-based medicine has in a comparatively short time become one of health care’s greatest growth industries. Everyone, it seems, now studies outcomes. Governments, professional groups, hospitals, insurance companies, managed care organizations, pharmaceutical companies, employers, and others are collecting data with the idea of monitoring or improving quality, reducing costs, and even rationing, or at least allocating, resources’; Kenneth Goodman, ‘Outcomes, Futility, and Health Policy Research’ in Goodman (ed), Ethics, Computing and Medicine (1998) 116 at 129.

19 See, eg. Christopher Mount, Christopher Kelman, Leonard Smith et al, ‘An Integrated Electronic Health Record and Information System for Australia?’ (2000) 172 Medical Journal of Australia 25. The authors argue that the health information system should (a) serve the health needs of both the individual and the nation; (b) enable the monitoring of trends, and facilitate health administration and management; (c) improve the efficiency of health service delivery, both personal care and public health services; (d) build from a primary care and population health base; (e) meet privacy and confidentiality requirements; and (f) should be developed intentionally rather than accidentally, in a coordinated rather than fragmented manner.
maximising the utility of health data for research purposes, where patients' identities can be protected.

**PART 1: Setting the Scene: Research Methodologies and Health Data Resources**

**A. The ‘Data Needs’ of Health Research Methodologies**

The uses of personal health information in health research are extremely varied. Lowrance helpfully summarises some of the different approaches to health research, noting that while such research generates new health data, it frequently proceeds by analysing data originally collected for clinical purposes.\(^{20}\) Table 1 below draws heavily upon, but interprets and slightly modifies, this analysis.\(^{21}\) There is considerable overlap between several of the research categories.

These approaches to health research encompass a broad spectrum of research methodologies. In some cases, researchers may have direct contact with patients personally; in others, clinical data alone may be sufficient, whether in identifying, coded (but re-identifiable), de-identified (anonymous), or aggregated formats. No attempt will be made here to provide a systematic review of the information needs that arise from different research strategies: a few examples will suffice.\(^{22}\)

An initial distinction can be drawn between the surveillance of patterns of disease and health status, and analytic studies (that is, those investigating causal relationships). In general, there is less need for researchers to have access to population surveillance data in name-identifying formats, although there are several exceptions. For example, notifiable diseases are generally reported on a

---


\(^{21}\) Although not stated by Lowrance, analytic epidemiology — research into the causes of disease — seems to fit best into Category 1 (the ‘biomedical science’ category), although the role of risk factors as contributing causes of ill-health, needs to be understood expansively, as encompassing social and environmental influences. Descriptive epidemiology — the monitoring of patterns of disease and health status within population groups — fits well within Category 2. While the scope of these terms is sometimes disputed, this is not a concern here.

name-identifying basis in order to avoid duplicate notifications, to facilitate contact tracing and (where necessary) emergency and even coercive responses to public health threats (see Table 1, categories 2–3). While data on the utilisation of health care services might be collected anonymously across population groups (Table 1, category 4), identifying data may be required in order to remind individuals to seek routine screening or care, or where researchers wish to follow patient groups in order to evaluate the outcomes of preventive actions and other interventions constituted by the patient’s interaction with the health care system. Similarly, while ‘outcomes’ research (Table 1, category 5), can focus on indicators of population health (for example, reduction in smoking prevalence following a targeted smoking cessation program), when individual health outcomes are of interest, it may be necessary to link clinical records, or data from health databases, using patient identifiers. Stanley points out that while the evaluation of health outcomes within the context of certain diseases might benefit from a total population database, the higher priority for epidemiologists is the capacity for strategic linking. Record linkage permits the identification and testing of relevant variables in an inexpensive manner; hypotheses can thereafter be refined in subsequent, and more expensive studies, such as surveys.

Identifying and investigating the relationships between risk factors and disease frequently requires researchers to accurately match longitudinal data relating to the same individual. As Sibthorpe and colleagues note, it is technically possible to identify individuals whose past experiences (exposures) or genetic risk factors may be relevant to their future health status and to follow them, in real time, using a variety of methodologies. In practice, this may be too expensive, impractical, and indeed unnecessary, since many of the indicators of health status that researchers are interested in are routinely recorded in clinical records, and reported to statutory or voluntary databases.

Case control studies are the most frequent kind of analytic study. In case control studies, persons with a particular disease or ‘health outcome’ (cases) are compared with a group of controls from a similar population who do not have the disease but who have been exposed at some point in the past, or over time, to factors thought to be risk factors for, or contributing causes of, the disease in question. By identifying factors that are present more or less often in cases, in comparison with controls, researchers aim to identify the relative risk constituted by those exposures in terms of how they increase or decrease the odds of developing the disease or condition. Thus, for example, researchers may investigate the relative risk of sleeping position, or of smoking (exposures) upon

---

23 Professor Fiona Stanley, Director, TVW Telethon Institute for Child Health Research and Professor, Department of Paediatrics, University of Western Australia; personal communication. 24 July 2000.
24 Beverly Sibthorpe et al. above n22 at 250.
Table 1: Forms of Health Research

<table>
<thead>
<tr>
<th>1. Basic biomedical research:</th>
<th>The science that underpins applied research; uses many experimental techniques, epidemiological techniques and forms of observation.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Studies metabolic mechanisms, hormonal controls, immune responses, conception, inheritance, development, cognition, memory, aging, abnormal functioning, including disease states, agents and risk factors affecting health.</td>
</tr>
<tr>
<td></td>
<td>Encompasses analytic epidemiology: the study of the causes of disease and the role of various risk factors.</td>
</tr>
<tr>
<td></td>
<td>Encompasses descriptive epidemiology: the monitoring and surveillance of events (such as patterns of hospital use, or HIV infection), including the prevalence and incidence of disease, and the development of vital statistics on births, deaths, and indicators of health status.</td>
</tr>
<tr>
<td></td>
<td>Reflected in notifiable disease reporting, the development of health statistics by government agencies, and various kinds of health data registries.</td>
</tr>
<tr>
<td>3. Research to reduce public health threats:</td>
<td>The monitoring of epidemics and other ‘emergency threats’ to public health (food poisoning, antibiotic-resistant infections, new strains of influenza).</td>
</tr>
<tr>
<td></td>
<td>Encompasses social science research (eg surveys of sexual behaviour).</td>
</tr>
<tr>
<td>4. Health services research:</td>
<td>Encompasses survey studies into attitudes shaping behaviour as it relates to use of health services (compliance with medication and treatment regimes; pap smears, breast examinations, prenatal obstetric examinations).</td>
</tr>
<tr>
<td></td>
<td>Source of data for evaluation of disease prevention and other interventions.</td>
</tr>
</tbody>
</table>
| 5. Evaluation research ('health outcomes' research): | - Encompasses the evaluation of treatments, clinical practices, health care services and public health programs in terms of their relative impacts and benefits, based on the observed 'outcomes' for patients, or within a defined population.  
- Examines large samples of real cases, using outcomes measures to inform the improvement of public health programs, clinical judgments (preferred drug combinations for AIDS patients, preferred strategy for smoking cessation programs), and the development of clinical practice guidelines ('evidence-based medicine').  
- Encompasses the analysis of pharmaceutical use in specific clinical settings, as well as the tracking of specific groups (patients with pacemakers, breast implants, blood donors), and quality of life surveys. |
| 6. Research into effective innovations: | - Includes research into the development and improvement of pharmaceuticals, medical devices, diagnostic instruments, vaccines, evaluating efficacy, risks, and cost/benefit, frequently through clinical trials. Such research is frequently a precursor to application for licensing of therapeutic products by the Therapeutic Goods Administration (TGA).  
- Encompasses post-licensing pharmacovigilance (watching for previously unknown effects of drugs, responding to adverse event reports), and post-marketing surveillance of patients. |
| 7. Economic analysis: | - Assessing the component costs of the health care system, including the costs of specific episodes of care.  
- Evaluating the cost-effectiveness of different ways of intervening in a resource-limited environment (eg prevention/education vs diagnostic programs vs treatment/management strategies). |
| 8. Market research: | - Encompasses research by commercial entities (eg pharmaceutical companies) into future projections of disease, prescribing patterns, markets for products under development.  
- Potential for closer relationship between commercial entities and patients as, for example, pharmaceutical companies form disease-management business supplying services directly to patients (eg diabetics). |
infant mortality within the first year of life (SIDS). Or they may calculate the relative risk of exposure to low levels of radiation (or proximity to high voltage power lines), by comparing exposure between groups of people with and without a disease.\textsuperscript{27} Case series studies may also assist in generating hypotheses about the causal role of various factors or exposures by identifying common features shared by a group of cases who also share the disease or outcome of interest.

In cohort studies, groups of subjects in different exposure categories are followed over time, to determine the proportion of patients who go on to develop the disease or health outcome. Researchers present their conclusions in terms of incidence rates of the disease or outcome between variously exposed subjects. Thus, for example, pregnant women in different age groups can be compared with respect to the rates of complications at time of giving birth, including caesarian sections and obstetric outcomes. Retrospective cohort studies, which involve the collection of records evidencing past exposure, such as employment records within a particular industry, may permit researchers to investigate the health outcomes of workers exposed to particular materials or toxins (for example, asbestos).

The methodologies described above are not unique to research investigating the causes of disease (analytic epidemiology). They may also be used in health services and health outcomes research. For example, researchers might study the role of breast cancer screening in older women in reducing the rates of mastectomies, by comparing the screening histories of women who underwent a mastectomy (cases), with those of women who were diagnosed with breast cancer but did not have a mastectomy (controls). Or they may investigate the putative causes of presumed adverse drug reactions in a particular patient population by comparing cases (patients who suffered the adverse reaction in question, for example, gastrointestinal bleeding), with a control group of people from that population, in terms of their medication history and current drug regime. Similarly, researchers might investigate whether kidney transplant patients suffer more frequent and serious complications when their hospital stay is reduced below a particular average length of time, by following a cohort of transplant patients who remained in hospital following surgery for varying periods of time.

Although cohort and case control studies can be carried out both prospectively, and retrospectively,\textsuperscript{28} they are almost always longitudinal,\textsuperscript{29} in that subjects are studied over time. This necessarily involves tracing the patient's clinical history for adequate evidence of exposures and outcomes. In case control studies, it may also be necessary to access patients' clinical histories in order to identify those who meet the definition of cases. The research methodology may involve interviews, surveys and other forms of contact with patients that also provide opportunities for obtaining permission to access and use data (although often this can only occur after some information has already been disclosed to researchers to enable them to

\textsuperscript{27} See Leon Gordis & Ellen Gold, above n22 at 155.
\textsuperscript{28} Andrew C Harper et al, above n25 at 105-106.
\textsuperscript{29} Ann Bowling, above n26 at 60.
contact the right people). In other cases, members of the patient group may be dead, incompetent, too distressed to approach, or untraceable. If such patients are excluded from the study (because they cannot consent), or if patients refuse to participate, the risk is that the overall sample will be biased.\(^\text{30}\) Even if patients are theoretically contactable, it may be prohibitively expensive or impractical to do so. This will be true where very large population groups are involved. From a scientific viewpoint, many studies can be conducted quite satisfactorily by linking data from clinical records, health databases and other sources (for example, employment records) to create a longitudinal record of past exposures, risk factors and disease outcomes. In these circumstances, the lawfulness of the research will revolve around the legal impediments to accessing data from these sources. This in turn will depend upon the four categories of 'constraint' identified previously,\(^\text{31}\) and the form of the information itself (whether identifying, identifiable, or de-identified).

### B. Health Databases and Sources of Health Research Data

In obtaining evidence of exposures and health outcomes, researchers will frequently seek access to data held in health registers and databases, as discrete repositories of information separate from clinical records. The issues surrounding access to data collections will frequently be similar to those surrounding access to clinical records. For example, the lawfulness of access to data contained in public hospital health records, and in a statutory database administered by a State Health Department, both depend upon State public sector controls. The distinction between clinical records and data registers is likely to diminish as health records gradually become databases: for instance, on-line collections of data, stored centrally or in distributed format, within networks that permit the searching and presentation of clinical data according to whatever variables are required.

Health databases take a variety of forms. As Lowrance notes, they may be organised by disease (for example, data on new HIV and AIDS diagnoses),\(^\text{32}\) by exposure, by mode of intervention, by general healthcare experience (for example, the hospital separations data within the inpatient statistics collection of each State),\(^\text{33}\) or by population. For regulatory purposes, a useful distinction can be drawn between statutory or government-administered databases, voluntary or non-statutory databases, and ‘in-house’ data collections.

---


31 These categories are: the duty of confidence at common law, statutory duties of non-disclosure, obligations under statutory privacy principles, and the ethical standards embodied in the National Statement.

32 The National Centre in HIV Epidemiology and Clinical Research at St Vincent's Hospital, Sydney, collates Australian surveillance data on HIV/AIDS, based upon reports of new HIV infections by pathology laboratories, and new diagnoses of AIDS by physicians.

(i) Statutory and Public Sector Databases

In Australia, as a result of limited federal constitutional powers, the provision of health services has traditionally been an area of State responsibility.34 Public health surveillance is primarily conducted by State and Territory health departments, which administer databases comprising data collected under mandatory reporting provisions in public health legislation.35 The legislative mandate to collect patient information means that the patient’s name and identifying details may be reported to Health Departments, thereby ensuring that these data are available for research, public health planning and other purposes.36 Public health legislation is not the only means of collecting health data from patients. Through public hospitals and other public-sector health services, State health departments collect inpatient statistics data37 and a broad range of other data required to fulfil ‘national minimum data sets’.38 Birth and mortality records are administered by the Registrar of Births, Deaths and Marriages39 (in NSW, birth and perinatal death are also notifiable conditions under public health legislation). Increasingly, information technology is facilitating the creation of broader, integrated population databases generated through database and record linkage, using (in the absence of a unique patient identifier) computer-assisted probabilistic methods to match patient variables.40

While health is primarily a State responsibility, the Commonwealth funds several major health programs, and accordingly, important national databases exist under Commonwealth law. These include the Medicare benefits database and the

35 See, for example the pap smear, birth, perinatal death, SIDS, cancer and neonatal birth defects registers established under the Public Health Act 1991 (NSW) and Public Health Regulation. See also. NSW Health, Strategy for Population Health Surveillance in New South Wales (December 1997).
36 HIV and AIDS are an exception. In response to the possible disincentives to HIV testing, Australian legislation generally requires coded notification of HIV diagnoses by laboratories, and of AIDS diagnoses by physicians; see, eg, Public Health Act 1991 (NSW) ss14, 17(1), and Public Health Regulation 1991 (NSW) s5; Health Act 1958 (Vic) s130, and Health (Infectious Diseases) Regulations 1990 s7 and schedules (as amended). See, further, Magnusson, above n8 at 400-401.
37 Above n33. In NSW, public sector sites report a variety of personal and clinical information on a name-identifying basis. Private sites are required by legislation to collect name-identifying information as part of the patient register (see Private Hospitals and Day Procedure Centres Act 1988 (NSW) s44 & Private Hospitals Regulation 1996 ss14–15). While the ISC is a sub-set of this register, patient names are not reported to the ISC. See, further, the circulars and resources linked at <http://www.health.nsw.gov.au/iasd/dm/isc/index.html>. Although the ISC is separation-based (ie, episode based, with the result that one hospital stay may involve, potentially, several episodes of care), NSW is moving towards client data linkage to permit the consolidation of records under a Universal Patient Identifier. See, further, Part 3.D below.
38 See below.
39 In NSW, see Births, Deaths and Marriages Registration Act 1995 (NSW) ss13, 17, 36, 42–43 & Births, Deaths and Marriages Regulation 2001. Legislation in other States is in similar terms.
Pharmaceutical Benefits Scheme (PBS) database. The Commonwealth also collects and administers census data.

Historically, wide disparities have existed between the content of State and Territory statutory databases. These include disparities with respect to what is notifiable under public health legislation, the content of the inpatient statistics collection, and differences between jurisdictions in the extent of their legislative mandate to develop data sets in target areas, or more generally. There are also continuing disparities with respect to the ‘release mechanisms’ that give researchers conditional access to these data sources. Some of the variation between jurisdictions in the content of statutory databases is slowly being smoothed out as a result of national agreement over ‘national minimum data sets’, although the rate of progress is a source of frustration for some researchers. A national minimum data set is a ‘core set of data definitions agreed by the relevant


41 The Medicare benefits database is administered by the Health Insurance Commission (HIC) under the Health Insurance Act 1973 (Cth). The Pharmaceutical Benefits Scheme (PBS) database is also administered by the HIC, under the National Health Act 1953 (Cth). Each database is functionally separate, and data can only be combined as permitted under Guideline 1.4 of the Medical and Pharmaceutical Benefits Programs Privacy Guidelines (issued under the National Health Act 1953 s135AA, and administered by the Federal Privacy Commissioner). The Guidelines were recently amended to permit data linkage with consent for the purposes of Coordinated Care trials. Other federal health databases include Australian Childhood Immunisation Register (established under the Health Insurance Act 1973 ss46A–46E), and the Hospital Casemix Protocol (HCP) Data Collection held by the Department of Health and Aged Care, pursuant to the 1995 Private Health Insurance Reform Legislation: see National Health Act 1953 s73AB; National Health Regulations 1954 Schedule 7 (Hospital Casemix Protocol).

42 See Census Act 1905 (Cth) ss12–13.

43 Some States have specific provisions enabling the development of specific data collections in particular areas. The Victorian Act, for example, constitutes a Consultative Council on Obstetric and Paediatric Mortality and Morbidity with powers to conduct inquiries into perinatal deaths and to conduct a perinatal data collection unit: Health Act 1958 (Vic) Part IXB. The NSW Act establishes a pap test smear register: Public Health Act 1991 (NSW) Part 3B.

44 In Victoria, for example, the Health Act 1958 (Vic) s9 requires the Secretary to establish a ‘comprehensive information system’ encompassing the causes and nature of illness in Victoria, and the utilisation of health services in that State’. In Tasmania, there is a generic power to set up ‘information registers’ and to require information for inclusion in the register to be reported to the Health Department: Public Health Act 1997 (Tas) s143. Neither of these kinds of provisions exist in the Public Health Act 1991 (NSW).

45 See Table 2, and Part 2.B below.
national information management group for collection and reporting at a national level'.

The National Health Information Agreement (NHIA), signed by Australian Health Ministers, the Australian Institute of Health and Welfare (AIHW), and the Australian Bureau of Statistics, provides a framework for the development of national health information in Australia. National minimum data sets developed through this process include national separation-based data on inpatients, mental health admissions, and palliative care, to name just a few. Agreement on definitions, standards and rules of collection, and the development of a National Health Data Dictionary are an important dimension of the NHIA work program, and provide the foundation for the collection of reliable and uniform health data. The reporting requirements for the national minimum data sets for institutional and other forms of health care impact, in turn, upon the information collection practices of public and private health care organisations. Typically, minimum data sets comprising ‘patient-level’ data consist of ‘identifiable’, rather than name-identifying data. Unique identifiers (called ‘person identifiers’) are a part of many minimum data sets which comprise ‘patient-level’ data. ‘Person identifiers’ will typically be an alphabetic, numeric or alphanumeric code unique to the establishment or health agency involved, and may be used for ‘episode linkage’.

The National Health Information Agreement (NHIA) is not the only national initiative for the development of national health data resources. Pursuant to the National Public Health Partnership, the National Public Health Information Working Group is working towards the implementation of the National Public Health Information Development Plan. The priorities of the Working Group


47 The National Health Information Agreement (NHIA) was signed in June 1993. In 1998 the agreement was extended to May 2003. The work program of the NHIA is coordinated by the National Health Information Management Group (NHIMG). See, further, ‘National Health Information Management Group: <http://www.aihw.gov.au/committees/health/healthmgmt.html>; House of Representatives Standing Committee on Family and Community Affairs, Inquiry into Health Information Management and Telemedicine, Submissions, Vol 1 at 75–82 (submission by the NHIMG).


50 Minimum data sets typically also include sex, date of birth, other demographic and health or welfare data relevant to that set, as well as an ‘establishment identifier’ (the agency or institution where the episode or event occurred). See n48 above.


include undertaking a national biomedical risk factor survey and a general social survey.

Both of these frameworks provide a context for the work of the Australian Institute of Health and Welfare (AIHW), a body established by Commonwealth statute in 1987, whose functions include the collection and dissemination of Australian health (and welfare) data.53 The AIHW receives data principally from State government and non-government agencies, and thus has an important role in making national health data available for research purposes.

(ii) Voluntary Databases

In contrast to statutory databases, voluntary collections are not the product of any government public health agenda. They typically reflect the clinical specialities and research interests of the principal collaborators, and may aim to compensate for the lack of accurate or adequate data from government and public sector sources.54 It is difficult to estimate how many such registers there are, although some have existed for many years.55 They range from modest, local initiatives to national databases, hosted by universities and research organisations, private and non-profit organisations, and even statutory bodies.56

It is important to note that just because a database is the product of voluntary reporting does not mean that it is a private sector database. The law that regulates the collection, use and disclosure practices of voluntary databases (as distinct from those of physicians reporting data to a database), will depend on whether the relevant data are hosted by a private sector organisation,57 or by a federal or State agency. Who exactly is the data custodian is not always clear. In some cases the administrative costs of a data register may be covered by private or by federal

53 The functions of the AIHW include collecting and producing health related information and statistics, conducting and promoting research into health, and providing researchers with access to health data subject to the legislation: Australian Institute of Health and Welfare Act 1987 (Cth) ss5-6. Similar powers exist with respect to welfare information, although powers of disclosure are more limited: compare s29(2)(c), and s29(2A).

54 See, eg; David A Ferguson, Geoffrey Berry, Tatiana Jelihovsky et al, ‘The Australian Mesothelioma Surveillance Program 1979–1985’ (1987) 147 Medical Journal of Australia 166 at 170. It is worth noting that the legislative mandate for notification of various data does not automatically ensure quality and timely data. Both statutory and voluntary data collections may suffer from under-reporting, uncertain diagnosis, and poor elucidation of risk factors and other indicators.

55 The Australia & New Zealand Dialysis and Transplant Registry (ANZDATA), for example, has existed since 1977 and contains data on over 13,000 patients. Certain genetic databases comprising family pedigree information on, for example, Huntington’s Disease, have existed for much longer.

56 The Australian Mesothelioma Register is one example, administered by the Research and Epidemiology Units of the National Occupational Health and Safety Commission (NOHSC), a Commonwealth agency set up by the NOHSC Act 1985 (Cth). The Epidemiology Unit of the Commission produces the annual Australian Mesothelioma Register Report. The register collects data on all new mesothelioma cases, without approaching the patient or next-of-kin, relying on voluntary notification by hospitals, clinicians, pathologists and cancer registries.

57 In this respect, there is little doubt that a health data register is a ‘health service’ within the terms of the Privacy Act 1988 (Cth) s6.
funding, or by a mix of funding from a variety of public and private sources, while the register itself may be located in a public hospital department. An analogy can be drawn with a public hospital that outsources, for example, its radiology services. In this scenario, the Privacy Commissioner’s health privacy guidelines suggest that the medical record would be subject to public sector legislation, since it would remain subject to ‘management by the public sector hospital’, despite the outsourcing. The same result would likely follow where there was a mix of funding sources supporting a data register administered by public health sector employees. Different considerations may apply, however, where a separate organisation is created and acts as custodian of registry data, or where a privately-funded database is separately administered from a public sector host institution, does not form part of the clinical record, and is located within a public agency simply for reasons of convenience or proximity to collaborating specialists. These and other possible ‘hybrids’ underscore the need for a national approach.

Like statutory registers, voluntary collections can play an important role in epidemiological and clinical outcomes research. The Australian and New Zealand Lung Volume Reduction Surgery Database, for example, permits comparison between ‘different approaches to patient selection, surgical and post-operative treatment’ in order to generate comparative data which will hopefully lead to improved patient outcomes. In the absence of a statutory mandate for the collection and sharing of patient data, however, issues of consent, confidentiality, compliance with privacy legislation and with the National Statement, all arise. In approaching these issues, the initial question, as noted above, is whether the database itself is subject to private sector or public sector controls.

(iii) ‘In-House’ Databases

Finally, voluntary and statutory databases can both be contrasted with ‘in-house’ registers. Hospital-employed and contracted specialists are frequently involved in research projects that run parallel with their clinical responsibilities. Not surprisingly, hospitals may host computerised databases with research applications that exist side by side with, or indeed as part of, ‘multi-function’ record systems that have no clear separation between therapeutic, research and managerial functions.

58 The Australian & New Zealand Dialysis and Transplant Registry, for example, is located in a South Australian public hospital, but is funded by the federal Department of Health and Aged Care, the Australian Kidney Foundation, the New Zealand government and grants from pharmaceutical companies. Funds are administered centrally through the hospital, which employs the four persons who administer the Register on a day to day basis. The executive who have overall control of the Registry are also public sector employees.


PART 2: The Current Legal Environment of Health Research

This part considers some of the practical questions that researchers, database administrators and physicians have about the collection, use and disclosure of health data, against the background of the ‘four layers’ of regulation identified previously (common law duties of confidence, statutory duties of non-disclosure, privacy legislation, and the National Statement). Section A considers the legal constraints upon ‘in-house’ research, by a physician who uses his or her patients’ health data for research that is unrelated to clinical care. Section B turns to research contexts that require access to ‘external’ data sources, reviewing the constraints that surround the administration of health databases, and the linkage of data from databases and clinical records.

A. ‘In-House’ Research

While it is beyond doubt that doctors owe their patients a duty of confidence, that duty is probably not breached when a clinician uses the patient’s data in research, even in the absence of patient consent. The law of confidentiality exists to enforce obligations of conscience arising from the circumstances in which information was communicated or obtained. As the trade secrets context illustrates, an obligation of conscience may not only prevent the unauthorised disclosure of information, but also its unauthorised use. In the medical sphere, however, the chief concern of the law is to protect patient privacy, and subject to maintaining patient anonymity, it seems reasonable for the law to foster the utility of information, including the use of patient data in medical research. This is consistent with the view that in protecting confidentiality, courts are enforcing obligations of conscience with respect to information, rather than any proprietary rights of the patient-confider.

61 To give just one example: the Austin and Repatriation Medical Centre in Melbourne is the largest hospital in Victoria. The Department of Respiratory Medicine at the Austin hosts databases on: (i) the respiratory laboratory (all people tested in the respiratory and sleep laboratories); (ii) raw data from sleep studies; (iii) details of all Department of Veterans’ Affairs and non DVA patients who have attended oxygen clinics; (iv) the Rehabilitation program; (v) a record of all VRSS (Victorian Respiratory Support System) patients who require home ventilation; (vi) appointments for all private physicians; (vii) a database of potential research subjects (patients in trials, considered for or interested in trials); and (viii) a database on individual research projects. The respiratory laboratory database, for example, includes the following details (not an exhaustive list): name, address, phone number, date of birth, height, weight, race, gender, Medicare number, insurance details, respiratory laboratory results, equipment used, billing, sleep laboratory reports, doctors letters, clinical notes, referrals, and the sleep laboratory waiting list. The databases fulfil several functions including storage of data, easy access to clinical notes, quality assurance and research. Source: Dr Christopher Worsnop, Department of Respiratory Medicine, Austin Hospital, speaking at session entitled ‘Ethical and Privacy Issues in Relation to Medical Databases Used in Research’, Thoracic Society of Australia & New Zealand, Annual Meeting, Convention Centre, Melbourne, 12 April 2000.

62 Slater v Bissett (1986) 69 ACTR 25 at 28 (Kelly J).


64 See, eg Smith Kline & French Laboratories (Aust) v Secretary, Department of Community Services and Health (1990) 22 FCR 72 at 92 (Gummow J), and (1991) 99 ALR 679 at 691 (full court).

65 See Breen v Williams (1996) 186 CLR 71 at 81, 90, 128–129; R v Department of Health, Ex parte Source Informatics Ltd [2000] 2 WLR 940 at 953; Smith Kline & French Laboratories (Aust) v Secretary, Department of Community Services and Health (1991) 99 ALR 679 at 691–692.
Imposing an 'obligation of conscience' upon the physician is not the same, therefore, as giving patients a common law right to veto the 'secondary uses' of their health data. In contrast to the constraints imposed by statutory 'information privacy principles', the limitations imposed by duties of confidence are relatively ill-defined. There is considerable doubt over whether the 'conscience view' of confidentiality would prevent physicians from exploiting the financial potential of patient health data to the exclusion of patients, in circumstances where there was no disclosure of identity. In R v Department of Health, Ex parte Source Informatics Ltd, the English Court of Appeal held that patients have no proprietary claim to the data contained in prescription forms and that anonymous (unlinked) data could be disclosed without patient consent to third parties for marketing purposes. Similarly, it remains to be seen whether patients themselves could impose an obligation of conscience upon physicians by expressly requesting that information only be used for clinical purposes. Since clinical data are increasingly the foundation of health care financing, patients are unlikely to be able to 'veto' the use of their data for financing and other managerial purposes. Even so, within the context of psychiatry, STDs or genetic testing, there may be strong public health justifications for wanting to enforce individual requests (and assumptions) that data remain 'quarantined' within the organisation and only used for the patient's clinical benefit. Furthermore, quite apart from concerns about privacy, even de-identified patient data can potentially be used to the detriment of ethnic, racial, sexual and other groups. Ultimately, the very flexibility of the 'good conscience' criterion suggests that the law of confidence can be adapted to prevent the causing of 'information-based harm' in variable circumstances.

Although breach of confidence law would rarely constrain physicians from using (as distinct from disclosing) their patient's clinical data for research purposes, it would nevertheless restrict access to the data to those health care providers who were directly involved in the patient's care. If identifying data were made available to a wider group (for example, a research group coordinated by the physician), that might itself constitute a breach of confidence. It is sometimes

---

67 Consider, eg, the patient data flows mandated by legislation for the purposes of casemix funding: National Health Act 1953 (Cth) ss73BD (hospital to private insurer), 73AB (private insurer to Department); Chris Maxwell, 'Casemix Perspectives for Clinicians in the Private Sector' (1998) 169 Medical Journal of Australia 48.
68 See Kenneth Goodman, above n18 at 133. Compare Coughlin, who argues that it would be unscientific to avoid asking questions about sexual orientation in large scale epidemiological studies, since (for example) lesbians may be at higher risk of breast cancer as a result of reproductive decisions, increased alcohol consumption and body mass, under-utilisation of screening mammography, and attitudinal, economic and provider-related barriers to receiving quality preventive health care: Steven S Coughlin, 'Ethically Optimized Study Designs in Epidemiology' in Steven S Coughlin & Tom L Beauchamp, Ethics and Epidemiology (1996) 145 at 148.
69 See van den Hoven, who argues that, quite apart from privacy, the prevention of 'information-based harm' provides the strongest justification for restricting access to medical records: Jeroen van den Hoven, 'Privacy and Health Information: the Need for a Fine-Grained Account' (2000) 12 International Journal for Quality in Health Care 5.
assumed that individuals who attend a health care organisation thereby enter into a relationship with all the health care functionaries who work there in a way that permits everyone to access the clinical record with impunity. The better view, however, is that only those health care workers who need to access the patient’s personal information in order to discharge their professional responsibilities have a right of access to it, and that other functionaries are effectively third parties for the purposes of the law of confidentiality.\footnote{This view makes sense, once it is recognised that a large hospital may employ or contract several thousand doctors, nurses, and other health care functionaries. In a large hospital environment, the patient’s ‘health care team’ (those involved in the patient’s care) may nevertheless extend to several hundred: M Stegler, ‘Confidentiality in Medicine: A Decrepit Concept’ (1982) 307 New England Journal of Medicine 1518.}

Increasingly, these common law constraints are being reinforced by privacy legislation. In common with other statutes, the private sector ‘National Privacy Principles’ distinguish between ‘primary’ and ‘secondary’ purposes. While the primary purpose of the collection of health information in a clinical context is the diagnosis and treatment of the patient, the use of the same information for research is regarded as a ‘secondary purpose’.\footnote{Privacy Act 1988 (Cth), Schedule 3, NPP 2.1(d); similarly, see the Health Records Act 2001 (Vic), Schedule 1, HPP 2.2(g).} The provisions permitting the collection, use and release of identifying patient information without consent are narrowly drafted and intended to act as a disincentive to this practice. A physician working in a private health care organisation is only permitted to use or disclose personal health information for ‘research, or the compilation or analysis of statistics relevant to public health or public safety’ where three requirements are satisfied. These requirements are that it is:

(i) impracticable to seek patient consent;
(ii) disclosure or use will be in accordance with ‘S 95A guidelines’; and
(iii) in the case of disclosure only, the organisation reasonably believes the recipient of the information will not on-disclose identifying information.\footnote{Privacy Act 1988 (Cth), Schedule 3, NPP 2.1(d). HPP 2.2(g) in the Health Records Act 2001 (Vic) is in similar terms.}

The ‘s 95A guidelines’ permit the use and disclosure of patient health information where a human research ethics committee (HREC) has determined that the research ‘outweighs to a substantial degree’ the public interest in protecting the privacy of the information.\footnote{National Health and Medical Research Council, Guidelines Under Section 95A of the Privacy Act 1988 (Draft – August 2001), para 4.2. As amplified by para 4.3, the ‘s 95A guidelines’ require a Human Research Ethics Committee to assess the degree to which:
• the research is likely to contribute to public health;
• the public importance of the research;
• the standards of conduct to be observed in the research;
• degree of risk of harm to patients; and
• to conclude that the public interest in the research use outweighs to a substantial degree the public interest in privacy: ibid.} Importantly, the National Privacy Principles, like
privacy principles in other statutes, only apply to 'personal information', which is defined as an information or opinion, whether true or not, about an individual 'whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

These constraints severely restrict 'in-house' research and data development, using identifying clinical information, in the absence of patient consent. Constraints upon use (as distinct from disclosure) of data for secondary purposes are a powerful way of protecting consumer sovereignty over health information, and of developing trust in the health care system. However, they come at a cost. Their effect is to degrade the utility of clinical data, even in circumstances where there is no risk of disclosure of data beyond the patient's immediate 'treating team'.

B. Legal Constraints to Data Linkage

The 'category-based' approach to health privacy is useful when considering whether researchers can lawfully access health data from clinical records in the custody of other health care organisations, from statutory and voluntary databases, and other sources. In addition, one must consider how these categories of regulation impact upon the development of health databases themselves. In the absence of a statutory duty to report, legal issues arise with respect to the initial reporting (that is, disclosure) of health data to a voluntary database by a 'reporting physician', as well as to the corresponding collection of that data by database administrators. As Table 2 illustrates, researchers seeking access to data from external data sources (for example, clinical records) effectively occupy the same position as a database administrator or other organisation soliciting clinical data from reporting physicians in order to build a health database. The ability of both parties to collect or to access the data will be constrained by any obligations of non-disclosure owed by the source of the data.

Table 2: The Relationship Between Collection and Disclosure Functions in Health Research

<table>
<thead>
<tr>
<th>Collection</th>
<th>Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researcher seeking access to data contained in clinical records held by another organisation, or in a statutory or voluntary database.</td>
<td>Constraints surrounding disclosure of health data by medical records administrator, database administrator, government agency, employer.</td>
</tr>
<tr>
<td>Voluntary database soliciting data from 'reporting physicians'.</td>
<td>Constraints surrounding disclosure of patient information by the reporting physician.</td>
</tr>
</tbody>
</table>

74 Privacy Act 1988 (Cth) s6.
(i) **Breach of Confidence and Data Linkage**

*Name-identifying data:* It is helpful to begin by considering how the common law constrains the source of the data from disclosing it — either to a researcher (for the purposes of record linkage), or to a voluntary database (for the purposes of developing a data collection). The data in question may be contained in clinical records, employer records, or a statutory or voluntary database. There is little doubt about the confidentiality of identifying information contained in clinical records. Releasing that data, without consent, either to a third party researcher who has no role in the patient’s treatment or care, or to a voluntary database, would constitute a breach of confidence, regardless of the social value of the research. Australian courts have taken a conservative view of the circumstances in which the public interest will justify disclosure of confidential data. While disclosure may be lawful in order to avert positive harm, it will not be lawful where disclosure is merely for some socially beneficial purpose.75

The requirement for consent may act as a disincentive to developing voluntary databases. One physician, responding to advice from a Human Research Ethics Committee that patient consent should be sought prior to releasing patient data to a research register, writes:

> It is hard enough getting medical information out of doctors, let alone getting them to prospectively get patients to fill out further paperwork. As a consequence of this, I think data will be very patchy indeed and distorting the whole picture.76

*De-identified data:* On the other hand, the law of confidentiality would not prevent the reporting of de-identified patient data to third parties, even in the absence of consent.77 An initial question concerns whether the data have really been de-identified in a way that preclude re-identification, whether by aggregation, or by the stripping of those identifiers that might, in combination, be used to match the data to an identity. A case in point is the code used in the National Cystic Fibrosis Database, which is based on the first two letters of the surname followed by the first two letters of the given name (the ‘2 X 2’ code).78 Where ‘anonymous’ data can nevertheless be linked to other identifying records on the basis of items common to both data sets (for example, the combination of date of birth, sex, postcode, and a numerical identifier), the data is clearly re-identifiable, rather than

---

75 See *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic) (1987)* 14 FCR 434 at 456, where Gummow J reinterprets the ‘public interest defence’ to mean that (only) information regarding ‘a crime, civil wrong or serious misdeed of public importance’ will lack the attributes of confidence needed to prevent disclosure to an appropriate third party. See also R Hayes, ‘Epidemiological Research and Privacy Protection’ (1984) 141 *Medical Journal of Australia* 621.

76 Confidential correspondence provided to the author.

77 See *R v Department of Health, Ex parte Source Informatics Ltd* [2000] 2 WLR 940 and nn62–64 above and surrounding text.

78 The 2 X 2 code is also required by statute for reporting HIV infection; above n36. The National Cystic Fibrosis Database is located at the CF Unit at the New Children’s Hospital, Westmead, Sydney. It contains genetic neonatal screening data for the 12–15 commonest genes causing Cystic Fibrosis.
de-identified. As Turkington intimates, legal controls for coded data need to take account of the capacity for digital technology to re-identify a specific source, despite the fact that such data may presently be non-identifying, since it is held separately from the identifiers in other data-sets that could facilitate identification. Ultimately, whether the disclosure of coded data represents a breach of confidence, or whether it constitutes 'personal information' (information from which the identity of an individual is apparent or could reasonably be ascertained) — thus attracting statutory obligations under privacy principles — is a matter of degree.

While public health surveillance, prevalence testing and the collection of group data on clinical outcomes may not depend on identifying data, de-identified data will be of limited value when the research methodology requires researchers to establish exposures, risk factors, or health outcomes in respect of individual patients. Speaking of the West Australian experience with record linkage, Jellie and Shaw note the increasing work undertaken on record linkage in order to 'develop a profile of clients and to estimate the number of individuals being served by a service or a group of services'. They note that data linkage techniques have been used 'to explore issues such as hospitalisation patterns over the last year of life, estimation of the incidence of hospital admissions for illicit drug problems, and to investigate suicide rates among admitted psychiatric patients'. Kelman and Smith argue that the inability to obtain access to identifying Census data, and PBS data, is a serious limitation of the WA 'Health Services Research Linked Database'. They also regret the fact that States de-identify hospital admissions data prior to making it available to the Australian Institute of Health and Welfare (AIHW) with the result that it is less useful for outcomes research.

_Coded, but re-identifiable data:_ This raises the question of whether it is possible to conduct data linkage studies using coded data. Some of the issues here can be explored by considering a hypothetical, prospective cohort study on patients with cystic fibrosis-related diabetes. A researcher who wished to identify CF patients with diabetes could obtain initial data from the National Cystic Fibrosis Database. However, that database only records information under code (a 3-digit code identifying the reporting hospital, together with a 2 X 2 code for the patient's name): the real identities of patients are held only by the reporting centres where they receive treatment. The disclosure of these coded identities to researchers would not, of itself, represent a breach of confidence owed to the

---

79 Richard C Turkington, 'Medical Record Confidentiality Law, Scientific Research, and Data Collection in the Information Age' (1997) 25 _Journal of Law, Medicine & Ethics_ 113 at 124.
80 See _Privacy Act 1988_ (Cth) s6; _Privacy and Personal Information Protection Act 1998_ (NSW) s9; _Health Records Act 2001_ (Vic) s3.
82 Ibid.
83 Kelman & Smith, above n22. See also n40 above.
84 Ibid.
85 Above n78.
patient, and would be necessary even if researchers intended to seek patient consent.

Armed with a list of coded identities, the researcher might then approach individual reporting centres for further data in respect of CF patients identified as having diabetes. The reporting centres might well refuse to cooperate with the study until a protocol were approved by the human research ethics committee of the reporting hospital or clinic, and until the patients had consented to being involved. Some patients, however, might be unable to give consent, or it might be impractical to contact them. To progress the study, without re-identifying the data, the researcher would need to rely on the reporting centre to extract data on the diabetes condition of cohort subjects and to make this available, under code. The need to rely on the goodwill and efficiency of the custodians of data is a complicating variable in epidemiological research.

As the study progressed, the researcher might wish to follow the clinical history of diabetic patients by accessing data stored at other ‘third party’ health care organisations they had accessed. Assuming the data held by the researcher remained under code, it would be necessary to find ways of accurately linking that data to the clinical data held by third party health services. In the absence of a universal patient identifier (UPI) common to both parties, this is not a straightforward exercise. Linkage would depend upon probabilistic comparisons between the remaining demographic identifiers in the researcher’s data set, and those held by the third party health service. Once probabilistic matching had occurred, researchers could then create their own numerical UPI to ‘identify’ the patient.

The National Statement draws a helpful distinction between the use of personal information to enable record linkage without consent (where identity is not revealed except to enable record linkage and is not retained thereafter), and broader disclosures of identifying or potentially identifying data. The National Statement permits human research ethics committees (HRECs) to authorise the transitory use of patient identifiers to form a longitudinal (but nevertheless non-identifying) record, where certain conditions are met.\(^86\) Thus, for example, the CF database code and related patient identifiers (for example, sex, date of birth, postcode) might be computer-matched on a probabilistic basis with the name-identifying record held by ‘third party’ health service providers. If this were an automated procedure, yielding additional data in respect of cohort subjects on a non-identifying basis, it might be possible to argue that no breach of confidence was involved. In some cases, however, the only feasible way of matching data would be to verify details of personal and health history.

This imaginary scenario illustrates the difficulties of trying to link data sets, in the absence of a UPI, while preserving confidentiality (by ensuring that researchers only ever had access to coded patient identities). One way of resolving

\(^86\) These are: (a) that the personal information permitting linkage is not retained after linkage; (b) that the identifying information is used with sufficient security; and (c) that the research has public benefit: ‘National Statement’. above n14, para 18.5.
these problems would be for the law to authorise disclosure of data to an independent ‘trusted third party’ or ‘honest broker’ (such as, for example, the CSIRO). The trusted third party would, on a cost-recovery or commercial basis, have transitory access to patient identities in order to conduct computerised data-matching and to prepare consolidated data in respect of individual patients. Consolidated data could then be made available to researchers, with patient identities remaining under code. Alternatively, data might be aggregated to a degree that was sufficient to suppress identity while still retaining geographic, age-specific, and other demographic data of interest to the researcher. If further information were needed by researchers, the ‘honest broker’ would again act as intermediary in verifying the identities of patients in order to accurately link records, and to prepare data under code for the researcher.

(ii) Statutory Duties and Data Linkage

The foregoing discussion shows that conducting research using coded, yet re-identifiable information, is surprisingly problematic, if the principle of confidentiality is taken seriously. Statutory duties, together with their exceptions or ‘release mechanisms’, further complicate the regulation of health data. As seen from Table 2, statutory duties constraining disclosure will apply (vis à vis the administrator of a voluntary database) to the ‘reporting physicians’ who contribute data to that database, as well as (vis à vis a researcher seeking access to identifying data) to a broad range of health data custodians.

There are several categories of legislation to take account of. Typically, health data held by State and Territory Health Departments are protected by non-disclosure provisions in health services statutes as well as statutes regulating, more specifically, public health. Although most of these duties apply to public sector organisations and health professionals, some also apply to the private sector. Interestingly, a recent survey of non-statutory registers in respiratory medicine found that six out of the seven specialist databases identified were hosted by a

87 Relevant State provisions include: Health Administration Act 1982 (NSW) s22; Public Health Act 1991 (NSW) s75; Mental Health Act 1990 (NSW) s289; Health Services Act 1988 (Vic) s141; Mental Health Act 1986 (Vic) s120A; Health Services Act 1991 (Qld) s63; Health Act 1937 (Qld) ss100E, 100F, 100I; Public and Environmental Health Act 1987 (SA) s42; South Australian Health Commission Act 1976 (SA) s64; Health Act 1911 (WA) s314 (applies to venereal disease information); Public Health Act 1997 (Tas) s147; Health Act 1993 (ACT) s21; Health and Community Services Complaints Act 1998 (NT) s23(1)(g) (breach of confidence a basis for complaint, as in other States). Legislative protections are largely non-existent in Western Australia, despite the fact it hosts Australia’s most comprehensive research linked database; above n40. Carter notes that ‘A committee appointed by the WA Minister of Health (the Committee) governs access to identifiable records on the database. The Committee determines applications on the basis of its view as to whether access would be in the public interest. Though the Committee claims it is cautious about granting access, there is no legislative framework governing either this database or more general research in WA’: Meredith Carter, ‘Protecting Consumers’ Interests in their Health Records’ (1999) 8(2) Australian Health Law Bulletin 13 at 15.

88 See, eg, Public Health Act 1991 (NSW) s17 (HIV/AIDS information); Health Services Act 1988 (Vic) s141 (applies to private hospitals); Health Act 1958 (Vic) s128 (HIV information); Health Act 1937 (Qld) s71B.
public sector organisation.89 Most statutes provide some sort of ‘release mechanism’, which authorises the release of identifying information to researchers for quality assurance activities,90 as well as for health research.

Secondly, the impact of freedom of information legislation, which exists in all jurisdictions except the Northern Territory, must be considered. Personal information protected by statutory privacy principles may, prima facie, be disclosed to third parties in accordance with FOI procedures.91 On the other hand, the release of a document that would involve the ‘unreasonable disclosure of personal information about any person (including a deceased person)’, is an exempt document.92 Health information is well recognised as a form of personal information,93 provided that identity is apparent or could reasonably be ascertained. Determining whether the disclosure of personal information is unreasonable involves a consideration of all the circumstances, and a balancing of the public interest in openness against the privacy interests of the information subject.94 Whether health researchers could use FOI legislation as a way of prising open patients’ public sector health records seems unlikely, despite the social value inherent in health research, given the strong corresponding public health interest in protecting confidentiality, as reflected in statutory duties of non-disclosure, and statutory privacy principles themselves.95 This conclusion is supported in those States where legislation provides that a document is exempt where its disclosure would found an action for breach of confidence.96 For these reasons, FOI legislation is unlikely to be an effective means of obtaining access to identifying or identifiable health information, although it could potentially provide an alternative access route for de-identified health data.

89 Frequently this was a public hospital department. The survey was conducted by Dr Christopher Clarke, above n15 (data presented by Dr Clarke and the author at the Australian Institute of Health Law & Ethics Annual Conference, Melbourne, 1 July 2001).
90 See Health Insurance Act 1973 (Cth) ss124C–124ZC; Health Administration Act 1982 (NSW) ss20D–20K; Health Services Act 1988 (Vic) s139; Health Services Act 1991 (Qld) ss30–38; South Australian Health Commission Act 1976 (SA) s64D(1)(b); Health Services (Quality Improvement) Act 1994 (WA); Health Act 1997 (Tas) s4; Health Act 1993 (ACT) Part III–III A.
94 See Re Chandra and Minister for Immigration and Ethnic Affairs (1984) 6 ALN N257 at N259 (Deputy President Hall).
95 See Re VXX and Department of Social Security (1992) 15 AAR 385; compare, however, Peter Bayne, above n91 at 18.
Thirdly, legislatures are increasingly enacting privacy statutes that impose ‘information privacy principles’ upon public sector agencies. Since 21 December 2001, large parts of the private sector have also been covered by the ‘National Privacy Principles’.\(^97\) In view of the trend towards health specific privacy legislation, provisions regulating the use of health information in research are split between generic, and health-specific, privacy statutes. The disclosure of ‘identifiable’ data to researchers, the disclosure of identifiable information to a health register, and the collection of such data by a register, arguably breach a number of relevant privacy principles.\(^98\) Table 3 below summarises some of the ‘release mechanisms’ that permit, as an exception to duties of non-disclosure, the release of data for research purposes, both at federal level,\(^99\) and in selected States. Clearly, no consensus emerges from this web of legislation in the way that State and federal bodies are required to balance health research with privacy considerations when determining access requests.

The ‘National Privacy Principles’ provide yet another model for determining the question of research access. As noted previously,\(^100\) private sector health providers are only permitted to use or disclose personal health data for research purposes when it is impracticable to seek patient consent, when the procedure set out in the ‘s 95A guidelines’ has been followed, and (with respect to disclosure), when the organisation believes that the recipient will maintain the confidentiality of the data upon release.\(^101\) Similar requirements also constrain the collection of such information in the first place, either by researchers collecting information about patients without their consent (perhaps in order to identify appropriate research subjects), or by database administrators (receiving data from reporting physicians). Collection without consent is permitted for public health research where the organisation could not achieve its purpose with de-identified data, where it is impracticable for the organisation to seek the patient’s consent to the research use, and where collection is in accordance with ‘s 95A guidelines’ approved by the Federal Privacy Commissioner.\(^102\)

Even where the NPPs permit the collection of data without consent, the organisation must thereafter take ‘reasonable steps to permanently de-identify the information before the organisation discloses it’ (NPP 10.4). Where collection is by a researcher for record linkage purposes, as in the example of researchers studying CF-related diabetes, this principle would prevent both on-disclosure and

\(^{97}\) Above n12.

\(^{98}\) Relevant provisions include the Privacy and Personal Information Protection Act 1998 (NSW) s8, 18 (applies to public sector agencies in NSW). Victoria and the ACT have health-specific privacy legislation that applies to both public and private sectors: see Health Records (Privacy and Access) Act 1977 (ACT) s5, Privacy Principle (PP) 10; Health Records Act 2001 (Vic) Schedule 1, Health Privacy Principle (HPP) 1-2 (but note the possible exceptions in HPP 1.1(d), HPP 2.2(g)). The Privacy Act 1988 (Cth) applies to Commonwealth agencies (see s14, IPP 11).

The private sector ‘National Privacy Principles’ are discussed below.

\(^{99}\) Above n41.

\(^{100}\) Above nn71–72.

\(^{101}\) Privacy Act 1988 (Cth), Schedule 3, NPP 2.1(d). See also Health Records Act 2001 (Vic) Schedule 1, HPP 2.2(g).
the publication of the data collected in identifying form. Where collection is by a database, however, NPP 10.4 would appear to make collection a 'once-off', thereby prohibiting administrators from on-disclosing that data in an identifiable form to researchers seeking evidence of (for example) exposure or health status information recorded in the database. The requirement to de-identify information acts as a serious limitation upon the utility of health databases. Of course, no problem arises where information is collected with patient consent.

Finally, it is worth considering the 'release mechanism' that applies to the disclosure of health information and statistics by the Australian Institute of Health and Welfare, given its key role in disseminating the product of national initiatives for the development of 'minimum data sets'. The release of information (including 'identifying' or 'identifiable' information) to researchers is authorised by statute where this has been specified in writing by the 'information provider' (for example, by a State health department, who reported the information to the AIHW), or where the Ethics Committee of the AIHW authorises the release in writing (where this does not contravene any written conditions upon which the information was first provided to the AIHW). It follows that the Institute's release practices will reflect any controls imposed by the information provider. Similarly, any researcher who seeks and obtains data from the AIHW will bear the same obligations of confidentiality as the AIHW itself. While the disclosure by a State agency to the AIHW of identifying compulsorily acquired health data would not constitute a breach of any common law duty of confidence owed to any

102 Privacy Act 1988 (Cth), Schedule 3, NPP 10.3. As an alternative to the third requirement, collection may be permitted where the collection is required by law, or 'in accordance with the rules of confidentiality issued by competent health or medical bodies', which bind the organisation. These requirements apply not only to collection for the purposes of research, or the compilation and analysis of statistics relevant to 'public health or public safety', but also to 'the management, funding or monitoring of a health service': ibid. Similar requirements apply to the private and public sectors in Victoria: Health Records Act 2001 (Vic), Schedule 1, HPP 2.1(e).

103 On the other hand, the argument might be made that NPP 10.4 was really only intended to apply in a record linkage context, in order to prevent information (collected without consent) from being disclosed in identifying form in research publications. There is some support for this in the commentary provided on NPP 10.3 in Office of the Federal Privacy Commissioner, Information Sheet 9, Handling Health Information for Research and Management (2001). In any event, NPP 10.4 is not well suited to a situation where a voluntary database is itself a source of data in a separate research project carried out by third party researchers.

104 Australian Institute of Health and Welfare Act 1987 (Cth) s29(2)(b)-(e). The AIHW notes, 'Typically, users of identifiable AIHW data are small teams of medical/health and social researchers who are usually attached to universities and/or associated hospitals. Increasingly, however, non university-based groups are taking an interest in research issues of public health importance. The main purpose of the research is frequently associated with the advancement of public health through the identification and/or control of determinants of ill-health, or the monitoring and evaluation of particular programs or procedures': AIHW, AIHW Information Privacy Review: Final Report, 1998, para 24.


106 Australian Institute of Health and Welfare Act 1987 (Cth) s29(3).
Table 3: Examples of Release Mechanisms in Australian Health Legislation Permitting Disclosure of Personal Information for Use in Medical and Epidemiological Research

<table>
<thead>
<tr>
<th>Legislation protecting privacy and confidentiality of government-held health data</th>
<th>Release mechanisms facilitating use of identifying health data in health research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cth</strong></td>
<td>Pursuant to Guidelines approved by the Privacy Commissioner under s 95 of the Act, federal public sector agencies may disclose personal information (contrary to the Information Privacy Principles (IPPs) in the Act) where a Human Research Ethics Committee has determined that the public interest in the research outweighs, to a substantial degree, the public interest in adhering to the relevant IPPs. Para 4A of the <em>Medicare and Pharmaceutical Benefits Program Privacy Guidelines</em> (issued by the Privacy Commissioner under the <em>National Health Act</em> 1953 s 135AA) permits disclosure of identifying claims information for research purposes if the individual consents or disclosure is in accordance with the ‘s 95 guidelines’. In addition, disclosures must also be authorised under the <em>National Health Act</em> 1953 s 135A, or the <em>Health Insurance Act</em> 1973 s 130. These provisions would permit disclosure for research purposes to a person who, in the Minister’s opinion, is expressly or impliedly authorised by the individual to obtain his or her data, or where disclosure is otherwise certified by the Minister to be in the public interest: NH Act s 135A(3); HI Act s 130(3).</td>
</tr>
<tr>
<td><strong>NSW</strong></td>
<td>S 23: Minister may, by order, authorise research into morbidity and mortality in NSW. <em>Health Administration Regulation 2000</em> s 13: Director-General may authorise disclosure of nominal health data required for the purpose of medical research carried out in accordance with NHMRC guidelines. <em>Public Health Regulation 1991</em> s 81A: Chief Health Officer may approve disclosure of epidemiological data to specified persons (presumably includes research purposes). Unlike the Privacy Act 1988 (Cth), the NSW Act lacks a statutory mechanism for authorising use of personal information in medical research. However, the <em>Draft Code on the Use of Public Sector Agency Records</em> (4 April 2001), para 4.2.3 would (if issued by the Minister under s 31) permit public sector agencies to disclose sensitive personal information (which would include health data) to an approved research project, provided the agency’s ethics committee complied with the criteria in National Statement.</td>
</tr>
<tr>
<td>Privacy Act 1988 s 14 (applies to personal information held by federal agencies)</td>
<td></td>
</tr>
<tr>
<td>National Health Act 1953 s 135A (applies to Medicare and PBS data)</td>
<td></td>
</tr>
<tr>
<td><strong>Legislation protecting privacy and confidentiality of government-held health data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Release mechanisms facilitating use of identifying health data in health research</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cth</strong></td>
<td>Pursuant to Guidelines approved by the Privacy Commissioner under s 95 of the Act, federal public sector agencies may disclose personal information (contrary to the Information Privacy Principles (IPPs) in the Act) where a Human Research Ethics Committee has determined that the public interest in the research outweighs, to a substantial degree, the public interest in adhering to the relevant IPPs. Para 4A of the <em>Medicare and Pharmaceutical Benefits Program Privacy Guidelines</em> (issued by the Privacy Commissioner under the <em>National Health Act</em> 1953 s 135AA) permits disclosure of identifying claims information for research purposes if the individual consents or disclosure is in accordance with the ‘s 95 guidelines’. In addition, disclosures must also be authorised under the <em>National Health Act</em> 1953 s 135A, or the <em>Health Insurance Act</em> 1973 s 130. These provisions would permit disclosure for research purposes to a person who, in the Minister’s opinion, is expressly or impliedly authorised by the individual to obtain his or her data, or where disclosure is otherwise certified by the Minister to be in the public interest: NH Act s 135A(3); HI Act s 130(3).</td>
</tr>
<tr>
<td><strong>NSW</strong></td>
<td>S 23: Minister may, by order, authorise research into morbidity and mortality in NSW. <em>Health Administration Regulation 2000</em> s 13: Director-General may authorise disclosure of nominal health data required for the purpose of medical research carried out in accordance with NHMRC guidelines. <em>Public Health Regulation 1991</em> s 81A: Chief Health Officer may approve disclosure of epidemiological data to specified persons (presumably includes research purposes). Unlike the Privacy Act 1988 (Cth), the NSW Act lacks a statutory mechanism for authorising use of personal information in medical research. However, the <em>Draft Code on the Use of Public Sector Agency Records</em> (4 April 2001), para 4.2.3 would (if issued by the Minister under s 31) permit public sector agencies to disclose sensitive personal information (which would include health data) to an approved research project, provided the agency’s ethics committee complied with the criteria in National Statement.</td>
</tr>
<tr>
<td>Privacy Act 1988 s 14 (applies to personal information held by federal agencies)</td>
<td></td>
</tr>
<tr>
<td>National Health Act 1953 s 135A (applies to Medicare and PBS data)</td>
<td></td>
</tr>
<tr>
<td>VIC</td>
<td><strong>Health Services Act 1988 s 141</strong>&lt;br&gt;(applies to 'relevant health services' in public and private sectors)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Mental Health Act 1986 s 120A</strong>&lt;br&gt;&lt;br&gt;<strong>Health Records Act 2001</strong></td>
<td>S 120A(3)(g): authorises psychiatric services to release information for use in medical or social research where this has been approved by the research ethics committee of the service.</td>
</tr>
<tr>
<td><strong>Health Privacy Principle 2.2(g)</strong></td>
<td>Health Privacy Principle 2.2(g) permits the use or disclosure of health information for research where it is impracticable to obtain patient consent, where non-identifying information will not be sufficient, where use or disclosure is in accordance with guidelines issued by the Health Services Commissioner, and the recipient will respect confidentiality.</td>
</tr>
<tr>
<td>QLD</td>
<td><strong>Health Services Act 1991 s 63</strong>&lt;br&gt;&lt;br&gt;<strong>Health Act 1937 s 100E</strong> (protects cancer registry information)</td>
</tr>
<tr>
<td></td>
<td>S 100E(3)(d): Chief Executive may release information to a person authorised by the Governor in Council under s 154M to conduct research into morbidity or mortality in Qld. Similar provisions apply with respect to the pap smear register and peri-natal information.</td>
</tr>
<tr>
<td>SA</td>
<td><strong>Public and Environmental Health Act 1987 s 42</strong>&lt;br&gt;&lt;br&gt;<strong>South Australian Health Commission Act 1976 s 64</strong></td>
</tr>
<tr>
<td></td>
<td>S 64D: the Governor may authorise a person to access confidential information for the purposes of conducting research into the causes of mortality and morbidity in SA.</td>
</tr>
</tbody>
</table>
individual, the legislative mandate to collect data implicitly imposes limitations upon the subsequent use of those data.\textsuperscript{107} Disclosure by a department for any purposes unrelated to those for which the statute originally authorised the collection of the data could be prevented by injunction,\textsuperscript{108} although this is an unlikely scenario where health data are disclosed for research, planning and other public health purposes.

The perceived ‘bureaucratic’ hurdles for accessing patient data held by government agencies represents a potential disincentive to the conduct of research using such data, and indeed, the reporting of such data in the first place. A review of privacy issues surrounding AIHW-held data noted that:

Anecdotal evidence suggests that some [users of AIHW data] become frustrated with delays in meeting their requests, with one or two citing Section 29 of the AIHW Act and the Privacy Act as major obstacles. Disgruntled with the perceived inability of the AIHW to satisfy their needs, they have even encouraged other potential clients of the AIHW to go elsewhere.\textsuperscript{109}

In summary, researchers conducting studies that require access to identifying patient data held by federal, State, Territory or private sector data custodians face a variety of release mechanisms based upon Ministerial or bureaucratic discretion, ethics committee consideration, or substantive statutory balancing formulas (Table 3). The sheer complexity of the legal framework illustrates the fragmentation of health privacy laws.

\textbf{C. The Fragmentation of Health Privacy Law}

\textit{(i) Problems and Misconceptions}

The discussion above reviewed the constraints upon health data flows in both the ‘record linkage’ context, and the ‘database development’ context, in both public and private sectors. The complexity of this web of legislation gives rise to both problems, and misconceptions. Firstly, the possibility of conflict between different statutory requirements operating \textit{within the one jurisdiction} is probably more apparent than real. For example, while the release mechanisms set out in the Health Records Act 2001 (Vic) HPP 2.2(g) and the Health Services Act 1988 (Vic) s141(3)(g) are clearly different (see Table 3), neither Act purports to provide an exhaustive statement of the circumstances under which health information may be disclosed. The former Act authorises the use of disclosure of health information for ‘secondary purposes’ where otherwise authorised ‘by or under law’ (HPP 2.2(c)), while the latter Act authorises disclosures under ‘this or any other Act’: s141(2)(c).

Secondly, the argument that State and federal privacy legislation merely creates ‘privacy principles’ enforceable through an administrative complaints regime, but does not otherwise alter the underlying duty of confidence, is flawed.

\textsuperscript{107} See \textit{Johns v Australian Securities Commission} (1993) 178 CLR 408 at 423 (Brennan J).
\textsuperscript{108} Ibid.
Parliamentary intention was surely that it would be lawful to disclose personal information in accordance with any exceptions to the relevant privacy principles; privacy legislation could scarcely be put into effect on any other basis.\textsuperscript{110}

More real, however, is the possibility of conflict between the (federal) National Privacy Principles and State laws applying to the private sector.\textsuperscript{111} State legislation that is inconsistent with a Commonwealth law will be invalid to the extent of any inconsistency.\textsuperscript{112} Under established principles, inconsistency can arise because of direct conflict between State and federal provisions, or because State legislation intrudes into an area where Commonwealth legislation is intended to ‘cover the field’.\textsuperscript{113} At first glance, the NPPs in the \textit{Privacy Amendment (Private Sector) Act 2000 (Cth)} set up a detailed framework for the collection, storage, use and disclosure of personal information that leaves little room for variant State legislation. On closer inspection, however, the NPPs do not appear to have been intended to codify the ways in which personal information (and health information) can be used. For example, NPP 2 permits personal information to be used and disclosed for purposes other than the primary purpose of collection where ‘the use or disclosure is required or authorised by or under law’.\textsuperscript{114} On the face of it, there seems no reason why a disclosure permitted under \textit{State} legislation (but not expressly under the NPPs themselves) would not suffice.\textsuperscript{115} If this interpretation is correct, then State legislation would remain valid in so far as it extended the categories of disclosure permitted by the NPPs. However, State legislation prohibiting the collection, use or disclosure of information in circumstances where this was nevertheless permitted under the (federal) NPPs, would fail on the basis of the ‘direct inconsistency’ principle.

(ii) The Causes of Complexity

This still leaves the problem of complexity itself, given the sheer variety of laws and ‘release mechanisms’ that operate in different States, Territories and sectors.\textsuperscript{116} There are several reasons for this complexity.

\textsuperscript{110} Compare Julian Savulescu, ‘Ethical Review of Record-Linkage Studies’, \textit{Australian Epidemiologist}, July 1999 at 6. Savulescu argues that a breach of confidence action might still be possible, even where disclosure was authorised as an exception to a statutory duty of non-disclosure. He argues that this possibility ‘represents an incentive for researchers to ensure breaches of confidentiality do not harm people. It is no more a disincentive to research than the possibility of a negligence suit is a disincentive to good medical practice’.

\textsuperscript{111} Consider, for example, the ‘release mechanism’ set out in the \textit{Health Services Act 1988} (Vic) s141(3)(g), as it relates to private hospitals, and the ‘National Privacy Principles’, above n12.

\textsuperscript{112} Under s109 of the \textit{Commonwealth Constitution}.

\textsuperscript{113} As Starke J said in \textit{Stock Motor Ploughs Ltd v Forsyth} (1932) 48 CLR 128 at 134, an inconsistency may arise because ‘the Federal power has set up a uniform and exclusive rule or code relating to a subject matter within its jurisdiction and no room is left for the operation of State law’.

\textsuperscript{114} NPP 2.1(g). NPP 10.1(b) also permits the collection of sensitive information (including health information) without a patient’s consent by an organisation where the collection is ‘required by law’.

\textsuperscript{115} Whether the reference in NPP 2.1(g) to uses or disclosures that are ‘required or authorised by or under law’ extends to uses or disclosures authorised under common law principles remains an open question, although the common law is less specific and any exceptions are likely to be reflected in existing statutory exceptions.
As noted previously, while federal privacy controls have grown up around the personal information generated through the two major Commonwealth-funded health programs (Medicare and the PBS), separate legislative frameworks protect the data holdings of each State and Territory. Traditionally, private sector health organisations were left to the common law, although this has changed with the coming into force of the National Privacy Principles. Secondly, State, Territory and Commonwealth provisions lack uniformity in their regulation of research access questions. In the record linkage context, the lawfulness of disclosure of data to researchers must be considered from the perspective of the law that applies to each potential discloser. Similarly, the collection, management or disclosure of data by a database will depend upon the mix of laws that applies in that jurisdiction, once it has been determined whether the database is subject to public or private sector controls. Statutes in some jurisdictions appear to lack an adequately sophisticated mechanism for balancing the public interest in privacy protection with the public interest in research. These discrepancies can interrupt multi-centre record linkage studies, or result in partial coverage within ‘national’ databases.

In addition to legal requirements, medical research in Australia is regulated through a decentralised process of ethics review, with human research ethics committees (HRECs) applying the standards set out in the National Statement. The National Statement facilitates multi-centre research by permitting HRECs to accept the scientific or ethical assessment of the ‘primary’ HREC monitoring a multi-centre project. However, participation in this ‘centralising’ process remains the prerogative of each individual HREC.

(iii) Can Law Help?

The fragmentation of health privacy law serves nobody’s interests. It makes good sense to move towards a national mechanism for regulating research access to health data in both private and public sectors. While a federally-imposed


117 Above n41.

118 For the factors that contributed to the Commonwealth’s decision to enact the private sector legislation, see Nigel Waters, ‘Commonwealth Wheels Turn Again — A Cautious Welcome’ (1999) 5 Privacy Law & Policy Reporter 127.

119 Consider, eg, laws in South Australia which require an instrument in writing signed by the Governor authorising the release of data to researchers (South Australian Health Commission Act 1976 (SA) s64D), compared to the more practical ‘release mechanisms’ requiring permission from the Director-General or Chief Health Officer (in NSW), or the approval of the relevant Human Research Ethics Committee (in Victoria); see Table 3.

120 National Statement, above n14, para 3.

solution, perhaps taking the form of a Commonwealth Health Privacy Act, is one possibility, any such legislation is unlikely to apply to health records generally.\textsuperscript{122}

Some measure of convergence is evident, however, in the 's 95 guidelines\textsuperscript{123} which operate in the Commonwealth public sector, in the National Statement, and in the 's 95A guidelines' that operate in the private sector.\textsuperscript{124} These sources suggest three criteria that may provide a more uniform mechanism for determining access requests to identifying patient data, in the absence of consent. Such data could only be disclosed without the patient's consent for research purposes where: (i) it would be unreasonable or logistically impossible to seek the patient's consent;\textsuperscript{125} (ii) where the research purpose underlying the collection or disclosure of data cannot reasonably be achieved except by using identifying or re-identifiable data; and (iii) where the public health interest in the research outweighs, in the circumstances, the patient's privacy interests to a substantial degree.

These criteria would determine whether a source of identifying data (contained in a database or clinical records) could release the data to a researcher, as well as whether a reporting physician could contribute to a voluntary register. The most obvious gatekeeper to apply these criteria with respect to research access requests would be a duly-established human research ethics committee (HREC). HRECs already service hospitals and other health care organisations, and in the federal sector, already apply the ‘section 95’ guidelines. HRECs are a cost-effective, practical and appropriate means of balancing competing public interests, especially in view of the ethical function served by laws regulating privacy and confidentiality.\textsuperscript{126} Some mechanism would need to evolve, however, to prevent the duplication, contradictory rulings and ‘HREC shopping’ that can occur under a decentralised HREC process, especially where access to data from multiple

\textsuperscript{122} However, the Commonwealth has foreshadowed specific legislation for electronic health records forming part of its HealthConnect strategy, in addition to a National Health Privacy Code which would bind participating providers: see ‘HealthConnect: June 2001 Update’: <http://www.health.gov.au/healthonline/connect.htm>.

\textsuperscript{123} National Health & Medical Research Council, Guidelines For the Protection of Privacy in the Conduct of Medical Research, approved by the Federal Privacy Commissioner under the Privacy Act 1988 (Cth) s95.

\textsuperscript{124} Above n73; see paras 3.6(f), 4.2.

\textsuperscript{125} As suggested by the National Statement, para 14.4(a), these requirement would be met where the procedures required to obtain consent would cause unnecessary anxiety to those whose consent was sought, or alternatively because the process of obtaining consent would prejudice the scientific value of the research, provided that (in either case) the research poses no disadvantage to the participants or to any collectivity involved. Alternatively, seeking consent may be impracticable due to the quantity or age of the records.

institutions is required. For large scale studies, applications might best be made at Area Health Authority, or even State, level.

As noted above, apart from a uniform ‘release mechanism’ for determining access to identifying data, health research would also benefit from laws designating and authorising an ‘honest broker’ or ‘trusted third party’ to temporarily access identifying data in order to link records and to create a consolidated, yet non-identifying health record for research purposes. This kind of initiative, as well as the development of model provisions harmonising data ‘release mechanisms’ within State and federal health legislation, would be an appropriate extension of the current ‘descriptive’ work being undertaken on confidentiality and privacy legislation by the Legislation Reform Working Group within the National Public Health Partnership.

PART 3: The Future Legal Environment of Health Research

One important assumption underlying health privacy laws is that health records should be ‘patient-centred’, in the sense that clinical data should only be used for the purposes of the patient’s own health care, except in exceptional circumstances. The obligations that secure this ‘patient-centredness’, together with numerous exceptions, add up to a complex web of regulation that has a constraining effect upon health research. This Part considers the regulation of health data flows and ‘research claims’ against the broader background of developments in information technology, health informatics, and health policy. It questions whether this ‘patient centred’ assumption in health care is consistent with evolving trends, and concludes with some modest proposals for how the design of electronic records systems might better facilitate health research, without needlessly jeopardising health privacy interests.

A. Health Informatics and the ‘New Public Health’

Despite the traditional assumption that the purpose of medical records is to assist the health care provider in managing the patient, there has been increasing interest in recent decades in the ‘secondary use’ of clinical information in public health surveillance and research. Developments in information technology and


129 Albrighton v Royal Prince Alfred Hospital [1980] 2 NSWLR 542 at 548–549 (Hope JA). This is reflected in the principles governing ownership of medical records: Breen v Williams (1996) 186 CLR 71 at 89 (Dawson & Toohey JJ).
health informatics have given further impetus to ‘secondary use’ claims. The increasing focus on information technology as a way of unlocking the value of clinical data to epidemiology and clinical outcomes research reflects what Lupton calls a ‘modernist’ approach to public health.130 In Australia, the rational development and strategic use of health data assets in public health is evident at the level of particular diseases, at the broader, clinical level, and at the level of public health policy generally.

At the level of specific diseases, although cancer registers, for example, exist in all States and Territories, there is an increasing focus on strategies to develop and use these data more effectively, in order to produce ‘indicators’ that will track the outcomes of clinical interventions, and facilitate a range of follow-on functions.131 Such a strategy requires the systematic collection of more patient information, from all points of contact with the health care system.132 At a broader clinical level, there is continuing interest in the use of record linkage techniques to create longitudinal patient histories (sometimes called ‘data warehouses’). These warehouses will facilitate evaluation of the effectiveness of treatments and health services, while also permitting researchers to monitor the occurrence of outcomes of interest across populations and over long periods of time.133 At a system-wide level, the National Public Health Information Development provides a platform for expanding the collection of several categories of public health data. These include data about the factors that influence the health of the population and the diseases it suffers from,135 data about the current health status of the population,136 and data about public health interventions and resulting ‘health outcomes’. The ongoing collection of data under each of these categories is

130 See Deborah Lupton, ‘A Postmodern Public Health?’ (1998) 22 Australian and New Zealand Journal of Public Health 3 (‘Modernity depends upon the notion that the key to human progress is objective knowledge of the world through scientific exploration and rationalised thinking and action’: at 3).
131 Hanna Noworytko, Helen Moore & Bruce Armstrong, ‘Towards a Clinical Cancer Information System’ (2001) 12 NSW Public Health Bulletin 28. These functions include monitoring patterns of courses of treatment by stage and other prognostic indicators; comparing treatment outcomes between centres; monitoring compliance with recommended practices; recruiting into clinical trials; and increasing communication between health providers.
132 Armstrong notes, for example, ‘Imagine a population-based cancer registry fed continually with individually linked data from warehouses contributed to by all, or nearly all, notifiers (such as hospitals and pathology laboratories). The data include information on in-patient and ambulatory surgical, chemical, biological and radiation treatment’: Bruce Armstrong, ‘The Future is Now: New and Better Cancer Information in NSW’ (2001) 12 NSW Public Health Bulletin 25 at 26.
134 Above n52.
135 This category of health data is referred to as ‘determinants of health’. It includes ‘physiological and behavioural risk factors and physical, social and economic environments’: id at 8. The determinants of health encompass structural determinants (indicators for measuring the social environment, socio-economic status, age and sex distribution, income distribution, education, and ethnicity), health hazards (eg, environmental data, food data, and indicators of tobacco, alcohol and drug use), and protective factors: id at 2.
required in order to determine the cost-effectiveness of various kinds of public health programs and interventions.

The transformational role of health informatics in health research is the result of at least two key influences. The first is the ‘new public health’. Goraya and Scambler point out that what is ‘new’ in the ‘new public health’ is ‘the rediscovery that influences on health are multifaceted and include economic, environmental, ecological, political and behavioural components, as well as the provision of, and equitable access to, medical services’. The ‘new public health’ (also referred to as ‘population health’) requires its practitioners to think beyond traditional assumptions about the ‘medical model of disease causation, diagnosis and treatment’. In contrast to the specialisation that characterises clinical care, there is growing realisation that health problems are ‘characterised by interdependence with one another, and by interdependence with life style and environment’. Richardson notes that, under the influence of the WHO definition of health, ‘there has been a transition in the conceptualisation of health from a clinical orientation to a greater focus upon the patient in a social context’. This is reflected in the Ottawa Charter for Health Promotion, which states that the role of the health sector ‘must move increasingly in a health promotion direction, beyond its responsibility for providing clinical and curative services’, and must ‘open channels between the health sector and broader social, political, economic and physical environment components’.

Information technology plays a key role in the ‘new public health’. Indeed, the information strategy of the ‘new public health’ finds logical expression in an integrated electronic health information network with the capacity to link data from clinical encounters, disease registers and other health databases, demographic data (for example, census data), environmental surveillance data and indices of socio-economic advantage, not to mention patient-reported data such as tobacco use, perceptions of ill-health or reasons for use of treatment services.

136 Health status data includes data on the incidence of diseases, injuries, adverse events, mortality data, biomedical risk factors such as body weight and blood pressure, and other self-reported life-style data. Id at 3, 6–8.


141 The WHO defines health as ‘a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity’: <http://www.who.int/aboutwho/en/definition.html>.


Anything less would fail to capture the significance of the lifestyle and environmental factors that — with the decline of infectious agents as major causes of mortality and morbidity — are key contributors to today's 'degenerative diseases'. Kirby points out that in population health informatics, 'the focus is on surveillance of the health status of entire populations, rather than simply on those who access services'. In addition, 'population-based health information systems are integrated with a variety of external data sources to provide a comprehensive perspective on the determinants of population health'. Since the databases that currently house these data are fragmented and separated by levels of government, commentators have emphasised the importance of unique patient identifiers (UPIs). By permitting the linkage of various data collections, UPIs facilitate evaluation of the outcomes of health care (at the clinical level), and of public health programs (at the level of population health). An outcomes focus, in turn, assists in determining best practice in health care and public health practice.

It is implicit in what has been said that the second key influence fuelling the growth of health informatics, and the associated trend towards 'secondary uses' of health data, is budget constraints and the imperative for a more efficient use of resources within the health sector. Spending on health care is slowly increasing, and the budget impact is expected to be magnified by the health needs of a growing, aged population. At the clinical level, Armstrong and Kricker argue that the chief value of record linkage to research into the outcomes of clinical interventions is that it generates feedback on health system performance. At the broader level of population health, there is keen interest in the development of 'public health indicators'; that is, measurements that reflect and can thus be used to monitor the performance of a public health program in achieving its objectives. The point of monitoring indicators of the impact and outcomes of a health program, Armstrong argues, is 'performance management'. Importantly, the National Public Health Information Development Plan envisages

144 Russell Kirby, above n139 at S18.
145 Kelman & Smith, above n22 at 101.
146 Ibid.
the cost-assessment of different kinds of public health strategy as responses to the same problem, in order to fix upon the most efficient allocation of resources.\textsuperscript{151}

These trends in the ‘strategic use’ of health data suggest that, over time, the demand for the ‘secondary use’ of patient data in public health and clinical outcomes research will intensify. The economic benefits of informatics and the potential gains to be derived from the ‘new public health’ will not only alter the nature of public health practice, but will transform clinical information systems and influence the assumptions that underlie current laws protecting health privacy.

B. Competing Frameworks for Regulating Health Data

The prevailing model for the legal regulation of health information is the ‘patient-centred’ model, which assumes that the primary use of health care records is the treatment and care of patients. Under a ‘patient-centred’ model, other uses of patient information (that is, ‘secondary uses’), are extraordinary, in the sense that they require special permission or some mechanism for mediating between the patients’ privacy interests, and the competing interests which favour ‘secondary uses’ (see Table 3). The National Statement is consistent with a patient-centred framework. It assumes that researchers begin their projects by devising a research protocol that identifies the information strategy appropriate to their work, with Human Research Ethics Committees (HRECs) performing a gatekeeper role when patient-identifying data is required.\textsuperscript{152} A feature of the ‘patient-centred’ model is that ‘secondary uses’, where justified, are limited and specific, rather than open-ended.

These assumptions sit uneasily with many of the ‘visions’ of a public health information system in the public health literature. Douglas, argues, for example, that:

The personal electronic health record, however it is stored and accessed, should also be the building block for ‘real time’ public health surveillance. Improved efficiency of personal clinical care and improved management of public health both require the same data and should become two sides of the one coin. When a patient presents for care by a general practitioner for a respiratory infection or a manifestation of HIV, that information should automatically become part of [a]

\textsuperscript{151} Australian Institute of Health and Welfare and the National Public Health Information Working Group, National Public Health Information Development Plan (1999) at 13–14. In other words, the measurement of health outcomes not only provides feedback on how to improve the delivery of a given program (operational efficiency), but it informs the decision whether to fund that program either at all or in priority to alternative ways of attempting to achieve similar public health objectives (allocative efficiency). Thus health promotion and disease prevention strategies are (just like treatment strategies) tested for efficiency in terms of health outcomes, within an environment where limited resources require governments and Health Departments to choose which of the range of strategies for tackling health problems in a population should be funded. See, further, Don Nutbeam, ‘Health Outcomes, Health Promotion and Improved Public Health in Australia’ (1995) 19 Australian Journal of Public Health 326; Gavin Mooney, Stephen Jan & Janelle Seymour, ‘The NSW Health Outcomes Initiative and Economic Analysis’ (1994) 18 Australian Journal of Public Health 244 at 245.

\textsuperscript{152} See the ‘National Statement’, above n14, paras 14, 18.
national public health monitoring activity. And when the laboratory reports to the GP that the respiratory infection is, or is not, a new strain of influenza that fact should, as well as informing the clinician instantly, feed into a national database that informs public health action.  

Having argued that all the clinical records relating to an individual should be linked to form a comprehensive, longitudinal ‘data warehouse’, Douglas adds that those records should become ‘instantly accessible building blocks for defined administrative, monitoring and research databases’.  

Similarly, Lowrance states that:

Outlining their vision for networked health care in the future, Hammond, Pollard and Straube write:

Finally, speaking in the American context, where a substantial component of health care services are delivered via employer-sponsored ‘care plans’, Dever argues that: ‘The opportunity for public health...is to link with managed care networks to provide population-based health information and measurement — a significant need of the managed care providers’.

These public health visions assume a ‘multi-function’ model of clinical records. Unlike the patient-centred model, researchers are not cast into the role of arguing for access to specified categories of data as an exception to the general rule which prohibits ‘secondary uses’. Rather, the unstated assumption is that what data

154 Ibid.
155 William W Lowrance, above n20.
are relevant for research purposes is an open-ended question that will change from
time to time and which depends fundamentally upon ongoing surveillance. Gone
is the old-fashioned ‘disease registry’, a central repository of data created through
the goodwill or statutory duties of the treating clinician. In its place is a health
information system with the capacity to generate databases on demand, to reflect
whatever parameters are desired, in accordance with the coding of clinical data in
the electronic patient record. In the multi-function model, public health shares an
equal status with clinical care.

C. Privacy and the ‘Multi-Function’ On-Line Health Care Record

This digital, ‘multi-function’ model of health records contrasts sharply with the
assumptions underlying Australian privacy legislation. Perhaps the most striking
contrast is the way that privacy principles constrain the purposes of collection, use
and disclosure of personal information. Limitations upon purpose are the measure
of patients’ control over their own health data, and they make patient consent a
central value in health care settings. The use of health data for inappropriate
‘secondary’ purposes, and the use of data, over time, for new purposes (a process
known as ‘function creep’) explain the suspicion with which privacy advocates
tend to view centralised databases. Examples of function creep in the health arena
include the use of confidential diagnostic data for criminal law purposes,158 and
the use of immunisation evidence as a pre-condition to receipt of social security
benefits.159 It is likely that the open-ended assumptions about the purpose of
collection of health data under the ‘multi-function’ model would infringe the
OECD ‘Purpose Specification Principle’, while the subsequent use of data for new,
‘secondary purposes’ would infringe the ‘Use Limitation Principle’, as reflected in
Australian privacy legislation.160

Despite the fact that digital networks may permit encrypted transmission, they
may also increase the seriousness of unauthorised data operations. While privacy
interests may be degraded in a hospital environment because dozens or hundreds
of functionaries may be involved in patient care and have a right to access the

158 See, eg, Clare Dyer, ‘Use of Confidential HIV Data Helps Convict Former Prisoner’ (2001) 322
British Medical Journal 633; Julian Savulescu, ‘The Myth of Confidentiality, the Patient’s
Good and Public Health’ Australian Medicine, 4 June 2001, 11 (data obtained in a research
study on HIV infection used to convict a participant for reckless transmission of HIV).

159 See A New Tax System (Family Assistance) Act 1999 (Cth) ss6, 39, 42.

160 The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
(OECD, Paris, 23 September 1980), were developed between 1978 and 1980 by the Expert
Group on Privacy chaired by Michael Kirby (now Justice Michael Kirby of the High Court). These
‘first generation’ privacy standards were highly influential in subsequent privacy
legislation enacted by OECD member countries, including Australia. The Purpose Specification
Principle states that the purposes for which personal data are collected should be specified at the
time of collection and subsequent use should be limited to those purposes. The Purpose
Specification Principle and the Use Limitation Principle are reflected, eg, in the Information
Privacy Principles that apply to the Commonwealth public sector (Privacy Act 1988 (Cth) s14:
IPP 2; IPP 10(1)(a); IPP 11(1)(a)); and in the National Privacy Principles (Privacy Act 1988
(Cth), Schedule 3, NPP 1.3; NPP 2.1).
A duty of confidence is nevertheless owed. The ‘very clumsiness and time consuming nature of the paper based system’ was itself a security safeguard. A networked electronic health care record, however, increases dramatically the number of health providers who will potentially have access to patient information. Increasingly, the risk of illegitimate access to data comes from those who are ‘authenticated users’ of the system. In the paper environment, patients could protect sensitive data (relating, for example, to psychiatric or sexual health), by ‘quarantining’ it within a particular health provider/patient relationship. In an on-line network, this facility would need to be explicitly built into the system. Indeed, computerised medical records may stimulate demand for ‘off-the-record’ care which will, in turn, affect the quality of on-line health data collections.

The ability to consolidate health data within an on-line health information network increases the overall sensitivity of any ensuing, longitudinal record. In comparison to an act of intrusion into a paper registry, one act of unauthorised access into a computer network may compromise the records of a much larger number of people, as well as more data relating to each individual. Finally, within a networked, ‘multi-function’ health record environment the ability to


163 As the Canadian Privacy Commissioner has observed, ‘[a] leak from a doctor’s office is damaging enough; maintaining a trusted relationship with the health system’s cast of thousands is quite another’: Canadian Privacy Commissioner, 1997/98 Annual Report at 4.

164 Recent examples include the case of an employee of the Health Insurance Commission detected browsing the records of women who had had IVF treatment, and Asian women: see ‘Health, Privacy and the New Technology’, The Law Report, ABC Radio, 27 February 2001; Lodkowski v Comcare (Federal Court of Australia, Goldberg J, 5 March 1998) (disclosure by an employee of the Health Insurance Commission that the applicant had had a termination of pregnancy prior to marriage); ‘MP’s Son Admits: “I Loaded Software”’ The Sun-Herald (2 September 2001); ‘Revealed: How MP’s Son Used Computer in Hacking Scandal’ Sydney Morning Herald (5 September 2001) (MP’s son loaded hacker softward on to his father’s Parliament House computer).


166 Commonwealth of Australia, Health On Line: A Report on Health Information Management and Telemedicine (Canberra: AGPS, 1997) at 94. Examples include Kaiser Permanente, a managed care organisation in the United States, which provides online services to members, which mistakenly sent 838 e-mail messages to the wrong recipients, some of which contained sensitive information; Janlori Goldman & Zoe Hudson, ‘Virtually Exposed: Privacy and E-Health’ (2000) 19 Health Affairs 140 at 141. In another example cited by Goldman and Hudson, thousands of patient records were accidentally posted on a public site at the University of Michigan Medical Center.
access, collect and download data may mean that there is no single, permanent ‘database’ containing specified data, under the control of any one entity. Data may simply travel as needed, between authenticated users of the system. In the absence of clear protocols regulating information transactions in this environment, it may be difficult to identify a specific ‘record-keeper’ upon whom the traditional responsibilities embodied within information privacy principles might be imposed.

Despite the risks inherent in the ‘multi-function’ model, health researchers point out that research claims should not be viewed with alarm since ‘[t]o researchers, the identity of the individual is irrelevant, except as a means of linking one set of information with another in order to identify factors influencing health outcomes’. On the other hand, Australian consumers regard their health data as highly sensitive, and evidence suggests that many have in fact lost the confidence of their health care providers, partly as a result of disclosures of health information without consent. It is well recognised that the success of current initiatives for a network of electronic health care records depends fundamentally upon the trust of consumers that their medical information will be adequately protected.

167 Beverley Sibthorpe et al. above n22 at 235.
168 Trish Crawford, ‘A Matter of Privacy’ Australian Doctor (19 March 1999) at 55. In a survey conducted by Mastercard, health records ranked behind financial transaction records as the category of data consumers were most sensitive about: ibid. On the other hand, there is some evidence that consumers would support the disclosure of health data for research purposes, provided researchers maintained confidentiality: Nigel J Gray, David Hill and Richard RH Lovell, ‘Privacy and Medical Research: Most People Support Current Practice’ (1990) 153 Medical Journal of Australia 740 (letter).
169 E Mulligan, ‘Confidentiality in Health Records: Evidence of Current Performance from a Population Survey in South Australia’ (2001) 174 Medical Journal of Australia 637. Mulligan reports that 9.6% of 288 survey participants were not confident that healthcare providers keep and use information responsibly. In the US context, Goldman and Hudson cite from a January 1999 Californian study that found that ‘one in six engage in some form of privacy-protective behavior to shield themselves from what they consider to be harmful and intrusive uses of their health information. Examples include withholding information from their health care providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and, in the most extreme cases, avoiding care altogether: Janlori Goldman & Zoe Hudson, ‘Virtually Exposed: Privacy and E-Health’ (2000) Health Affairs 140 at 141.
D. **HealthConnect and Other Government Initiatives.**

While Australian privacy legislation, with its emphasis upon the informed choice of the patient, is consistent with a 'patient-centred' model of clinical records, can the same be said of current government initiatives for the development of electronic health records? Furthermore, to what extent do existing health privacy laws constrain these new initiatives?

(i) **National Initiatives**

At a national level, the development of a networked health care environment is occurring through the National Health Information Management Advisory Council (NHIMAC), established in July 1998 by Australian Health Ministers, and bringing together consumers, and representatives of Australian governments and the private health sector. NHIMAC is the peak body advising Health Ministers on the most appropriate framework for implementing a national approach to information technology management within the health sector. Following on from its November 1999 report, *Health Online*,\(^{171}\) the National Electronic Health Records Taskforce was established by Health Ministers through the Council. In its July 2000 report, *A Health Information Network for Australia*,\(^{172}\) the Taskforce assessed the benefits and difficulties of a national approach to electronic health records, and proposed key features of a network of electronic health records, now known as HealthConnect.\(^{173}\)

While the exact architecture remains uncertain, HealthConnect would involve the systematic collection of health and demographic data at point of care. Such data would be stored as episodic, event summaries, in an agreed format, and would be stored in a distributed manner.\(^{174}\) For example, hospital and pathology event summaries might be held on-line at the relevant hospital, while general practitioner records might be stored at regional level. Such data would be available to authorised users and could be assembled in different ways.\(^{175}\) The principal benefit of the network would be improved continuity and quality of care resulting from the ability of all linked health providers to access and share up-to-date patient information.\(^{176}\) In addition to improved productivity and cost savings within clinical care,\(^{177}\) electronic health records would support clinical and health

---

171 Above n170.
172 Ibid.
173 HealthConnect was referred to as HINA (Health Information Network Australia) in the Taskforce report. For updates on the progress of HealthConnect, see <http://www.health.gov.au/healthonline/connect.htm>. Electronic health records are not the only on-line health initiative arising from the Health Online Report. See also the Better Medication Management System (BMMS), above n13.
174 'Event summaries would include such things as: basic information about the outcome of health interventions; a hospital discharge report or referral; a summary of pathology investigations; and other summaries that health care providers generate now': 'National Electronic Health Records Taskforce Report', above n170 at 120.
175 Id at 120.
176 Id at 168–169.
177 Id at 170–177.
services research through the linking of clinical databases and the development of population-based approaches to public health surveillance. The Taskforce noted that new uses of data, and new contributors of data, might emerge over time.

The Taskforce noted the tension between confidentiality and the accessibility of health records, but emphasised that patient consent would be a pre-requisite to the participation of his or her data within the network. This is clearly the case, since the very process of calling up a patient’s health record would give health providers access to information generated about the patient in separate clinical contexts and organisations. In the absence of consent, or specific statutory authority the act of accessing data could constitute the knowing (and unlawful) receipt of confidential information. The Taskforce noted that patients who agreed for their data to participate in the network would also indicate the purposes for which their data could be used at the time they registered with the network (with regular prompts to providers to reaffirm or influence patients’ preferences). Patient participation ‘may range from not agreeing to automatic contacts for preventative procedures to allowing all research agencies access for research purposes. Some consumers may wish to control very specifically each individual process’.

Exactly how consumer control over health data might be implemented is far from clear. It is possible that each individual patient could determine (and the system could enforce) the passwords, alphanumeric identifiers and/or demographic data required to confirm that patient’s identity, and to provide a health care worker with access to that patient’s electronic health record. Once uniqueness is established, the partitioning of the health record remains another option for ensuring that the entire clinical record was not necessarily accessible to all authorised health providers. Again, it is technically possible that every data item entered on-line could be matched to a graded series of ‘authorisers’, with additional passwords or identifiers being required to access particularly sensitive categories of data. Similarly, different parts of the medical record might be linked to different levels of research access, with more elaborate ‘release

---

178 Id at 49, 69, 97. The Taskforce notes that ‘Population data collection is potentially useful to society through research and analysis. The costs of interfacing the various health departments’ computers with provider systems and processing provider data should drop if a national approach to electronic health record systems and standards were adopted’: id at 97.
179 Id at 129.
180 Id at 77, 121, 164.
181 See Attorney-General v Guardian Newspapers (No 2) [1990] 1 AC 109 at 268 (Lord Griffiths).
183 ‘National Electronic Health Records Taskforce Report’, above n170 at 77; see also at 125.
186 Shoenberg & Safran, above n184, note that ‘Different combinations of authorisers are possible for different categories of medical information, so that a dynamic matrix of authorisation requirements can be tailored for the granular content of the record. Naturally, the requestor is unaware of the process of identification and authorisation for data access is simply returned with data items for which he or she has satisfied the security requirements’. 
mechanisms' operating for more sensitive categories of data (for example, genetic data). On the other hand, the extent to which individuals could segregate aspects of their record or impose idiosyncratic access requirements is likely to be constrained by arguments focusing on clinical necessity, administrative burden, and the economic and public health benefits of administrative and research access. Despite the technical possibilities, there will be strong pressure for each patient record within a system like HealthConnect to operate according to a standardised, rather than individually tailored, protocol.

Many features of the HealthConnect architecture remain to be determined. These include the possibility of a 'confidentiality override' to permit authenticated health providers to access the on-line record in emergencies, and the technical challenges of migrating data to new computer systems throughout the life of the patient. The Taskforce acknowledged that the transfer of data between sites would be secured by encryption, within a national Public Key Infrastructure, and that clear guidelines for audit trails would be required. To assure unambiguous identification of an individual patient across the health care system, and large-scale record linkage for population health research and policy development, a unique health identifier would be required.

The emerging legislative framework for privacy protection within HealthConnect has three layers. As foreshadowed in the Taskforce report, the National Privacy Principles would apply to private sector organisations participating in HealthConnect. Secondly, a 'National Health Privacy Code', to be developed through public consultation, would bind both public and private sector health providers participating in the network. Thirdly, the Taskforce noted that further legislation may be necessary to specify how a universal health identifier would be protected, to regulate data-matching activities, and to specify the permitted uses of health information held within HealthConnect. These second and third layers would ensure a uniform, national approach to the privacy of on-line data. The Taskforce envisaged an access control body that would oversee the network, exercising functions similar to those of the Federal Privacy

187 Kenneth D Mandl et al, above n3.
189 Id at 76, 135. For a useful discussion of the functional specifications required for electronic health records to support the provision of care and the transfer of data across health care institutions, see David M Rind, Isaac S Kohane, Peter Szolovits et al, 'Maintaining the Confidentiality of Medical Records Shared Over the Internet and the World Wide Web' (1997) 127 Annals of Internal Medicine 138.
190 'National Electronic Health Records Taskforce Report', above n170 at 96, 98, 108, 140. The Taskforce appeared to favour the introduction of a unique number identifier based on the existing Medicare card and Health Insurance Commission identifier: ibid Appendix H. The Medicare number is already used both for the receipt of Medicare benefits, and more recently, pharmaceutical benefits: see National Health Amendment (Improved Monitoring of Entitlements to Pharmaceutical Benefits) Act 2000 (Cth).
192 Above n170 at 135.
193 Above n12.
Commissioner. These functions would include determining the access claims of researchers and planners to health data, monitoring access arrangements, investigating complaints and enforcing statutory penalties for breach of access rules.\(^{194}\)

Despite this framework, doubt remains over whether patient data could be drawn from electronic health records without consent, for research and other applications.\(^{195}\) While most research and planning is expected to rely on de-identified data,\(^{196}\) the Taskforce notes that 'separate legislative approval' may be needed for large scale record linkage of identifying data for population health purposes.\(^{197}\) The Taskforce was also equivocal over whether patients could 'opt out' of contributing their health data to an electronic record.\(^{198}\) As these factors illustrate, although strong privacy protection is a selling point for participation in the network, the data required by governments for public health surveillance and planning, and in order to see a return on their investment in on-line networks, suggests that some rationalisation of privacy is inevitable.

(ii) NSW Initiatives

The development of HealthConnect has not prevented State-based initiatives for electronic records, and New South Wales is taking a leading role.\(^{199}\) In its March 2000 report, the NSW Health Council recommended the introduction of both an electronic health record (EHR) and a unique patient identifier (UPI), as part of a broader set of recommendations to capture the benefits of information technology

---

195 The Taskforce states: ‘Researchers studying particular diseases are likely to be one of the few groups wanting access to identified data. Procedures will need to be developed to handle such requests and provide appropriate safeguards. Consumers will need to be reassured that the procedures and protocols will be in place to provide an adequate level of assurance’: id at 95.
196 Id at 121–122.
197 Id at 97–98.
198 Ibid. Compare p 164 & Appendix F at 7. In December 2000, the NSW Advisory Committee on Privacy and Health Information noted that 'It appears that what is emerging at the Commonwealth level is a combination of a 'compulsory' and 'voluntary' model. That is, it is compulsory for every person to be registered, but voluntary as to what information is included on the electronic network. However, the true extent to which the proposal is voluntary or compulsory remains unclear': NSW Advisory Committee on Privacy and Health Information, Report to the NSW Minister for Health, 'Panacea or Placebo? Linked Electronic Health Records and Improvements in Health Outcomes', December 2000, <http://www.health.nsw.gov.au/policy/gap/privacy/epreidency.pdf> (hereafter ‘NSW Ministerial Advisory Committee Report’) at 30–31.
199 Mr Chris Puplick, the NSW Privacy Commissioner, has noted that a national electronic system could take years to develop, and in view of the need to obtain States’ and Territories’ support, would probably result in a ‘lowest common denominator’ approach. He notes that a NSW system could set ‘higher and better standards for privacy than the Commonwealth’: ‘Electronic Files to Hold Medical Records', Sydney Morning Herald, 30 January 2001 at 1. This paper does not attempt to review initiatives in other States. In Victoria, the Primary Care Partnership initiative encompasses the development of electronic health records: see Department of Human Services (Victoria), Primary Care Partnerships: Information Management Strategic Directions, March 2001 at 30–32: <http://hnb.dhs.vic.gov.au/acmh/phkb.nsf>.
in the health sector.\textsuperscript{200} Those recommendations are in the process of implementation as part of the NSW Information Management and Technology Strategy (IM&T). By June 2003, the UPI is expected to be implemented at the Area Health Authority level, moving towards a State-wide identifier thereafter. The NSW EHR, now known as EHR*NET is expected to be rolled out progressively and to be closely aligned with HealthConnect. EHR*NET would link hospitals, general practice, and other community point-of-care clinical systems and would include "an event summary comprising client demographics, clinical information, outcomes of care and an ongoing management plan".\textsuperscript{201}

In its December 2000 report, the NSW Ministerial Advisory Committee on Privacy and Health Information noted that the "linking of electronic health records cannot proceed without gaining the confidence of the public that the introduction of such a system is in their best health interest and does not present unacceptable risks to privacy".\textsuperscript{202} Contrasting EHR*NET with the somewhat equivocal status of HealthConnect, the Advisory Committee stressed that a NSW system must be an "opt-in" system giving patients the right to exclude their data from automatic transfer,\textsuperscript{203} backed up by audit trails.\textsuperscript{204} In view of the fragmentation of privacy legislation within NSW, the Advisory Committee unanimously recommended health specific privacy legislation covering electronic records, covering both public and private sector bodies, overseen by the NSW Privacy Commissioner.\textsuperscript{205}

The Advisory Committee noted that EHR data will be "highly valued for health research purposes", and that the "ability of linked EHRs to potentially provide a cradle-to-grave record has been highlighted as one of the key advantages of the EHR system".\textsuperscript{206} Conscious, perhaps, of the limitations of an "opt in" method in facilitating research access, the Committee recommended that research access to linked electronic health records should be mediated according to the "section 95 and 95A guidelines".\textsuperscript{207} The Committee recommended against commercial access to de-identified or aggregated data without permission from NSW Health and the Privacy Commissioner.\textsuperscript{208} More generally, the NSW Privacy Commissioner would retain a broad jurisdiction with respect to EHRs.


\textsuperscript{202} ‘NSW Ministerial Advisory Committee Report’, above n 198 at 17.

\textsuperscript{203} Id at 30–32, 40.

\textsuperscript{204} Id at 19, 43.

\textsuperscript{205} Id at 24–25.

\textsuperscript{206} Id at 41.

\textsuperscript{207} Id at 41–42. It remains to be seen what role HRECs would have in determining whether ‘s 95/95A’ criteria were satisfied. While local HRECs monitor studies that relate to patients or data within their organisation, it is not yet clear whether EHRs would be implemented according to a highly distributed, rather than a centralised, system: id at 27.

\textsuperscript{208} Id at 42–43.
Conclusion

It may be tempting to think, given a reading of HealthConnect and EHR*NET reports, that tomorrow’s electronic health record may succeed in being both a ‘multi-function’ and a ‘patient-centred’ repository, and that the dichotomy between a ‘multi-function’ and a ‘patient-centred’ health record, is a false one. This conclusion may be premature. What we are witnessing is the early stages of a ‘political sell’. Privacy protection is the selling point of a health information system that must respond to budget constraints, to the information needs of the ‘new public health’, and to higher levels of usage of health services by aging ‘baby boomers’. This does not mean that electronic health records are a bad idea, nor that the coordinated (‘seamless’) care facilitated by health care networks will not benefit consumers, and improve ‘health outcomes’.

 Australians have a highly developed sense of privacy, and in the health arena they may (with some justification) adopt a cautious approach to the benefits of consolidated, on-line records.209 It remains to be seen whether the ‘patient-centred’ rhetoric surrounding HealthConnect and EHR*NET will withstand consumer indifference to the benefits of linked records, minimal ‘opt in’ rates (and thus a poor return on the massive investment required to develop health networks), or a tendency among consumers to authorise highly variable and ‘edited’ versions of their health care record in different contexts. The factors motivating the massive investment in health informatics, ‘population health’ and associated ‘secondary use’ claims are almost certainly likely to water down the level of ‘individualised’ control individual patients might wish to exercise over the distribution of their health data.

While the special risks posed by integrated, on-line health records might justify retaining an ‘opt-in’ framework, the costs of such a system are likely to mean that some level of participation will become compulsory. A ‘gold standard’ of privacy might give patients unlimited control over what consultations, or parts of consultations, remained off-record. Realistically, however, patients will not be able to negotiate on an ad hoc basis with their health providers about the security and accessibility of their data. Instead, privacy solutions must take the form of standardised procedures built into the system itself that permit the partitioning of particularly sensitive categories of information (for example, sexual health, mental health, genetic counselling, sexual abuse and adolescent health data). In order to minimise the disincentives to seeking treatment, it would also be important for patients to be able to direct that certain clearly defined categories of data remained off-line, or to require their specific consent to be obtained before any health worker accessed that data category. Importantly, these ‘options’ would be part of the architecture of the system, and available to every patient.

To implement a ‘multi-function’ health records system that permitted researchers to access on-line data without consent would be to institutionalise

209 See Meredith Carter, above n126 at 161–162, discussing the Creutzfeldt-Jakob disease (CJD) saga involving the Health Insurance Commission, and the trade in personal information uncovered by the NSW Independent Commission Against Corruption (ICAC).
breach of confidence (the knowing receipt of confidential data from other health care contexts), as well as the breach of privacy principles in some jurisdictions (through the use of such data for secondary purposes without consent). Against this background, two broad issues arise for debate. Firstly, to what extent is it possible to exploit the utility of health data, and to facilitate longitudinal linkages for research purposes, without compromising patient confidentiality? While legal recognition of 'trusted third parties' might provide a temporary solution, in the digital age, unique patient identifiers are perhaps a more efficient, and enduring, solution.

In March 1996, former Federal Privacy Commissioner Kevin O'Connor observed that:

It is almost inevitable that with the desire to track people through the health system over time (to provide better coordinated care and also to provide information on outcomes, for planning and for research) that there will be renewed calls for a unique identifier in the health system. It is no accident that the development of a national patient identifier has been singled out as a high priority by the National Health Information Management Advisory Council (NHIMAC) overseeing the development of HealthConnect, and is central to the development of EHR*NET. Researchers themselves continue to call for one.

A function-specific, unique patient identifier-for-research (a UPI-R), implemented as part of an on-line health information system like HealthConnect or EHR*NET, may provide the best possibility for broader, yet privacy-sensitive access to longitudinal health data for research purposes. If given a genuine level of control over what data participates in the on-line network, patients might choose to associate individual clinical encounters with a UPI-R, at point of care. Even better, if health research really does lead to improved health outcomes and efficiencies, it would make sense to create strong incentives (perhaps through the level of the Medicare rebate at each consultation) to encourage patients to consent to the linking of their health care encounters with a UPI-R. By opting to associate their clinical data with the UPI-R, patients could be assured that research access would be on an anonymous basis, rather than on an identifying basis (as at present, pursuant to the release mechanisms summarised in Table 3). One advantage of storing HealthConnect data in a distributed format would be to combat the perception that the network would generate centralised medical histories on individuals for vague or unknown government purposes. Under the current

210 See nn71–72 above and surrounding text.
211 Kevin O'Connor, above n162 at 7. Commissioner O'Connor went on to note that unique patient identifiers (UPIs) are a 'two-edged sword from a privacy perspective' in that while they may assist in ensuring the accuracy of the data attributed to a person, a multi-purpose UPI can act as a key for linking 'vast amounts of information held in a variety of places (government and non-government) about an individual', and for developing profiles: ibid.
213 Beverly Sibthorpe et al, above n22 at 253; Kelman & Smith, above n22 at 101.
proposal, UPI-R-linked data would simply reside within the system, permitting longitudinal linkage with data from other UPI-R-approved clinical encounters. This would largely dispense with the necessity for a ‘trusted third party’ to link data to form a consolidated data set.

The linkage of clinical encounters with a UPI-R facilitates data linkages without sacrificing confidentiality. Since the health information network would ‘exist’ for the purposes of clinical care, researchers would need to obtain ethics approval for their research, and to seek authority from the authorised ‘gatekeepers’ for access to specified categories of on-line, UPI-R-linked data. Guidelines for determining how this might occur within a distributed network, and criteria for use in scrutinising access requests, could be issued by the federal Privacy Commissioner, or other access control body exercising similar functions. Within a distributed network, the administrative burden of scrutinising requests for research access to on-line data, in accordance with the guidelines, would be sensibly borne by human research ethics committees (HRECs) representing the various ‘gatekeepers’, or designated custodians, of the various caches of data. Thus, for example, if general practice and pathology data were stored at Area Health Authority level (in NSW), access requests could be administered by the HREC for that Area.

Since people generally access health care services using their names, the linking of a UPI-R to clinical data at point of care does not itself deliver patient anonymity, but only the possibility of anonymity, provided that name, address and (in certain circumstances) other identifiers were stripped away before data were made available to researchers. One benefit of having an HREC scrutinise access requests to UPI-R-coded data would be to ensure that functional separation was maintained between patient identities, and UPI-R-linked data, or between the treatment and research function. Researchers who satisfied the requirements applied by the gatekeeper (as administered by the HREC applicable to that gatekeeper), and paid for the administrative costs involved in the data manipulations inherent in the gatekeeper role, could obtain access to data sets identified only by, and linked by, the UPI-R. Subject to fulfilling the requirements for research access, researchers could follow patients across the health care system, through their UPI-R-linked clinical encounters. Given that statutory privacy principles also place limitations upon physicians from using their own patients’ clinical data for research purposes,214 physicians who wished to study their own patient population, and to link their health data without consent, would also need to step back from the treatment function, and seek access to UPI-R-linked data, through the relevant HREC.

This is only one of many possible ways of implementing a unique patient identifier for research within an on-line network. The obvious benefit of a UPI-R is that it serves as a substitute for identifying information when linking data to generate longitudinal records. The gatekeeper role, oversighted by the applicable regional HREC, would ensure that researchers only received UPI-R-identified

214 See NPP 2.1(d); above n72 and surrounding text.
data. The cost and administrative burden of the gatekeeper role, under the current proposal, might well be less than what would be required if, for example, the gatekeeper role involved rendering patient records irreversibly anonymous through non-reversible encryption of patient identifiers, prior to delivering the relevant data set to researchers.\(^{215}\)

The second issue that arises for debate is: what should be done if patients are generally reluctant to associate their data with a UPI-R? On one response, it might be necessary for researchers to seek the assistance of ‘trusted third parties’ to link records (if the law permitted this), or to satisfy the requirements of existing ‘release mechanisms’ that permitted access for research purposes without consent. As Gold notes, however, balancing privacy interests with the public interests flowing from health research is not unique to epidemiological research. In other contexts, society has made its compromises, from the reporting of sexually transmitted disease on a name-identifying basis, to requiring individuals to be vaccinated.\(^{216}\) Since the widespread use of a research-specific UPI could ensure the anonymity of patient data in the hands of researchers, the public interest arguably favours the compulsory linkage of data to a UPI-R, in order to maximise the utility of that information. On the same basis, it might be appropriate to extend the use of a UPI-R beyond the clinical record to include births, deaths, Medicare and PBS data.

---


216 Ellen B Gold, ‘Confidentiality and Privacy Protection in Epidemiologic Research’ in Steven S Coughlin & Tom L Beauchamp, *Ethics and Epidemiology* (1996) 128 at 129. See also Leon Gords & Ellen Gold, above n22 at 156 (‘the social contract that facilitates the existence of individuals within social groups requires that each individual occasionally yield some of his rights, including privacy and freedom of action, for the benefit of society as a whole’).