Australian Government

Office of the Privacy Commissioner

# Explanatory Statement

# Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs

**Issued under section 135AA of the *National Health Act 1953***

**Issued on 6 March 2008 to take effect on 1 July 2008**

# Explanatory statement for the Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs

This explanatory statement has been drafted for the purpose of fulfilling the Privacy Commissioner's obligations under section 26(1) of the *Legislative Instruments Act 2003.*

## 1. PURPOSE AND AUTHORITY

The instrument creates new binding guidelines concerning the handling by Australian Government agencies of information obtained by any agency in connection with a claim for a payment or benefit under the Medicare Benefits Program and the Pharmaceutical Benefits Program ('claims information'). The Privacy Commissioner is required to issue such guidelines under section 135AA(3) of the *National Health Act 1953* ('National Health Act').

The Guidelines are legally binding and ensure that claims information is linked and used only for limited purposes and in particular circumstances. A breach of the Guidelines constitutes an interference with privacy under section 13 of the *Privacy Act 1988* ('Privacy Act'). In turn, an individual may complain to the Privacy Commissioner about an alleged interference with their privacy. Sections 3 and 4 of this Explanatory Statement give more detailed information on the operation and effect of the Guidelines.

### Authority for making the Guidelines

The authority for making the Guidelines, and the requirements as to the matters they must deal with, are prescribed in subsections 135AA(3) to (5) of the National Health Act. These subsections provide:

> (3) The Privacy Commissioner must, by written notice, issue guidelines relating to information to which this section applies.
>
> (4) At any time, the Privacy Commissioner may, by written notice, issue further guidelines that vary the existing guidelines.
>
> (5) So far as practicable, the guidelines must:
>
> (a) specify the ways in which information may be stored and, in particular, specify the circumstances in which creating copies of information in paper or similar form is prohibited; and
>
> (b) specify the uses to which agencies may put information; and
>
> (c) specify the circumstances in which agencies may disclose information; and
>
> (d) prohibit agencies from storing in the same database:
>
> (i) information that was obtained under the Medicare Benefits Program; and
>
> (ii) information that was obtained under the Pharmaceutical Benefits Program; and

(e) prohibit linkage of:

(i) information that is held in a database maintained for the purposes of the Medicare Benefits Program; and

(ii) information that is held in a database maintained for the purposes of the Pharmaceutical Benefits Program;

unless the linkage is authorised in the way specified in the guidelines; and

(f) specify the requirements with which agencies must comply in relation to old information, in particular requirements that:

(i) require the information to be stored in such a way that the personal identification components of the information are not linked with the rest of the information; and

(ii) provide for the longer term storage and retrieval of the information; and

(iii) specify the circumstances in which, and the conditions subject to which, the personal identification components of the information may later be re-linked with the rest of the information.

The full text of sections 135AA and 135AB are at Attachment A.

Issuing the Guidelines is also a function of the Privacy Commissioner under section 27(1)(pa) of the Privacy Act:

27 Functions of Commissioner in relation to interferences with privacy

(1) Subject to this Part, the Commissioner has the following functions:

...

(pa) to issue guidelines under section 135AA of the *National Health Act 1953*;

## Relevant provisions of the *Privacy Act 1988*

Personal information is defined in section 6 of the Privacy Act as:

> … information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Notably, the information to be covered by these Guidelines is defined in broader terms than the definition of 'personal information' in the Privacy Act. This is discussed below under section 2 of this Explanatory Statement (see 'Information regulated by the Guidelines').

In making these Guidelines, the Privacy Commissioner has taken account of the matters required by section 29 of the Privacy Act. That section states that the Privacy Commissioner, in the performance of his or her functions, and the exercise of his or her powers, shall:

> (a) have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the recognition of

the right of government and business to achieve their objectives in an efficient way;

(b) take account of:

(i) international obligations accepted by Australia, including those concerning the international technology of communications; and

(ii) developing general international guidelines relevant to the better protection of individual privacy;

(c) ensure that his or her recommendations and guidelines are, within the limitations of the powers of the Commonwealth, capable of acceptance, adaptation and extension throughout Australia; and

(d) ensure that his or her directions and guidelines are consistent with whichever of the following (if any) are relevant:

(i) the Information Privacy Principles;

(ii) the National Privacy Principles;

(iii) the Code of Conduct and Part IIIA.

### Other relevant legislation

The secrecy provisions set out in section 130 of the *Health Insurance Act 1973* ('Health Insurance Act') and section 135A of the National Health Act prescribe rules around the handling of information collected in the course of the activities of both the Department of Health and Ageing ('the Department') and Medicare Australia. In making these guidelines, the Privacy Commissioner considered the effect and interaction of these provisions.

# 2. REASONS FOR MAKING THESE GUIDELINES

## Background to the Guidelines

The National Health Act was amended in 1993 by the *National Health Amendment Act 1993* to introduce section 135AA and section 135AB. The then Privacy Commissioner first issued guidelines under those sections on 24 November 1993, which came into effect on 15 April 1994.

Section 135AA(3) creates a statutory requirement for the Privacy Commissioner to issue these Guidelines. Section 135AA also sets out a number of matters with which the Guidelines must deal.

These Guidelines are also intended to implement the findings of the review of the previous guidelines made under section 135AA. The Office of the Privacy Commissioner ('the Office') published its *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS claims information* ('Review Report') in August 2006. This report is available on the Office's website at www.privacy.gov.au.

## Information regulated by the Guidelines

The information to which the Guidelines apply is determined by subsection 135AA(1) of the National Health Act, as information that:

(a) is information relating to an individual; and

(b) is held by an agency (whether or not the information was obtained by that agency or any other agency after the commencement of this section); and

(c) was obtained by that agency or any other agency in connection with a claim for payment of a benefit under the Medicare Benefits Program or the Pharmaceutical Benefits Program.

Section 135AA(2) expressly excludes from the regulation of the Guidelines:

- information relating to the providers of goods and services about which the claim was made;
- information in a database that is maintained for the purpose of identifying individuals who are eligible for entitlements under the two benefits programs; and
- information that is not stored in a database.

The difference between information regulated by the Guidelines and information regulated by the Privacy Act is worth noting. The definition of 'personal information' for the purposes of the Privacy Act only covers information from which an individual's identity is apparent or reasonably ascertainable.

In contrast, the Guidelines apply to a broader category of information that 'relates to' an individual, by virtue of section 135AA(1). The Privacy Commissioner believes that information that 'relates to' an individual need not necessarily identify that individual. In this way, claims information that is stripped of its "personal identifying components"[1] would still fall within the scope of the Guidelines (though may not, in such circumstances, be regulated by the general provisions of the Privacy Act).

In the Commissioner's view, subsection 135AA(5)(f) of the National Health Act expressly reflects that the Guidelines should apply to this broader category of information. This provision requires that the Privacy Commissioner make guidelines regarding how information stripped of personal identifying components is to be handled, notwithstanding that such information would not ordinarily be covered by the Privacy Act.

# Issues considered in making the Guidelines

### Policy intent of the legislation and guidelines

The policy intent of the enabling provision for the Guidelines, section 135AA of the National Health Act, is to recognise the sensitivity of health information and restrict the linkage of claims information. Such linkages may reveal detailed information on the health status and history of the majority of Australians, beyond what is necessary for the administration of the respective programs. As discussed further below, it should be noted that provision remains for the use of such information for health policy and medical research purposes in certain circumstances.

[1] This is a term defined in section 135AA(11) to include such information as name, address and Medicare number.

The purpose of the Guidelines is to give effect to section 135AA of the National Health Act. The Guidelines provide specific standards and safeguards for the way that individuals' claims information is handled by Australian Government agencies when stored in computer databases. These standards are in addition to any requirements that may be imposed by the Information Privacy Principles ('IPPs') contained in section 14 of the Privacy Act.

The primary objectives of the Guidelines are to ensure the separation of claims information collected under the Medicare Benefits Program and the Pharmaceutical Benefits Program, as well as establishing the circumstances under which this information may be linked and retained in linked form. The Guidelines also prescribe the circumstances in which claims information may be retained in various forms, such as where it is required to be separated from personal identifying components (that 'de-identified'). The establishment of regular reporting requirements and a framework for limited retention periods is intended to ensure that the linkage and retention of claims information does not result in the de facto combination of the two databases.

### Commissioner's responsibilities under section 29 of the Privacy Act

In making these Guidelines, the Privacy Commissioner has met the statutory obligations to give regard to certain matters set out in section 29 of the Privacy Act. These include giving due regard to important social interests that may compete with privacy, as well as the right of Government to achieve its objectives in efficient ways.

In particular, the Privacy Commissioner has considered the potential value of claims information being used for health policy and health research purposes. Accordingly, the provisions relating to these purposes remain largely unaltered from the previous Guidelines.

In regard to the efficiency of Australian Government agencies' objectives, the Privacy Commissioner has made changes from the previous Guidelines following submissions from relevant agencies. These changes reduce unnecessary administrative burdens while ensuring that adequate privacy protections are retained. These changes are reflected primarily in Guidelines 3 to 5, described in detail in sections 3 and 4 of this explanatory statement.

## Matters raised during consultation

The Privacy Commissioner's decisions in making these Guidelines were substantially informed by the 35 written submissions received during the consultative process, as well as by subsequent detailed consultations with stakeholders. The consultation process is described in section 5 of this explanatory statement. The key issues and considerations raised during this process are set out below, and are discussed in further detail in the Office's August 2006 Review Report, available at www.privacy.gov.au.

### Sensitivity of health information

A number of stakeholders emphasised the sensitivity of the information in question, arguing for the retention of robust protections for its handling. Some

stakeholders pointed to the potential for individuals to be stigmatised or discriminated against if their claims information (which in many cases may disclose the relevant underlying condition) was handled inappropriately.

In particular, submissions from a number of consumer, privacy, health ethics and peak professional bodies claimed that the purposes for which claims information from the two benefits programs may be linked should be kept relatively narrow.

A number of submissions noted that some suggested additional uses for claims information might be met by other means, thus negating the need to expand the purposes for which claims information from each benefit program may be linked.

The Privacy Commissioner agrees that the information in question is, generally, likely to be of a type that the community would expect to be handled with special care. Further, it was found that the level of protection afforded by the previous guidelines was generally appropriate and should be reflected in the new Guidelines.

### Medical research

Submissions from stakeholders with an interest in medical research claimed that it was important that the claims information from the two benefits programs be available for medical research. A number of submissions pointed to the need to permit claims information to be linked for medical research purposes.

The Privacy Commissioner agrees that there is a strong public interest in claims information being able to be used for medical research, subject to appropriate protections. However, it was noted that the previous guidelines expressly provided for this purpose. The Privacy Commissioner has also noted that the relevant prohibition against linking claims information extends only to Medicare Australia; it is beyond the authority of the Guidelines to restrict how researchers outside of the Australian Government handle claims information (though other provisions, such as the general obligations of the Privacy Act, may apply).

Accordingly, the provisions concerning medical research in the Guidelines remain largely unchanged from the previous instrument (see new Guideline 6). The Privacy Commissioner has, however, noted that further education and information on how the Guidelines apply to medical research may be helpful.

### Efficiency in government administration

The Privacy Commissioner noted submissions from the Department and Medicare Australia that the previous guidelines created unnecessary administrative burdens.

For example, Medicare Australia, the Department and a number of other submitters supported Medicare Australia being able to retain ‘old’ claims information for longer than the previous prescribed period of five years.

Medicare Australia and a number of other submitters also supported an extension to the three-month fixed period for which Medicare Australia may retain linked datasets of claims information. However, it was noted that these supporting submissions were based on using the linked datasets for medical research. In the Office's Review Report, it was noted that Medicare Australia is not permitted to link claims information for the purpose of medical research. While other external researchers may conduct such linkages, these will not be covered by the 3-month retention period.

It should also be noted that a number of other submissions either supported the three month retention period, or advocated that it should be shortened.

The Privacy Commissioner is satisfied that some of the obligations established by the previous Guidelines imposed unnecessary administrative and regulatory burdens on Medicare Australia and the Department, as well as being potentially inconvenient to individuals. The clearest example of this has been the need for Medicare Australia to retrieve 'old information' from the Department to provide a report to individuals of their claims history. Providing individuals with such a report can be delayed by the need to retrieve this information from the Department.

The Privacy Commissioner is further satisfied that alternate measures could be established to ensure appropriate protections around how claims information is linked, without imposing unnecessary administrative burdens. These measures are codified in new Guidelines 3, 4 and 5, and these remain consistent with the statutory requirements and policy intent of section 135AA.

# 3. GENERAL OPERATION AND EFFECT OF THESE GUIDELINES

### Legal status of these Guidelines

The Guidelines are legally binding on Australian Government agencies and ensure that claims information is linked and used only for limited purposes and in particular circumstances.

The Guidelines ensure that the sensitive health information contained in databases holding claims information is appropriately managed and protected. This protection accords with the legislative intent of section 135AA of the National Health Act. The protection afforded by the Guidelines applies in addition to the protection given to personal information under the Privacy Act.

In some instances, the Guidelines set a higher standard of protection for claims information than that required under the Privacy Act and deal with issues not covered by the Information Privacy Principles (IPPs) in the Privacy Act, including by specifying obligations concerning the retention, de-identification and the destruction of claims information. Guideline 9 clarifies that the Guidelines prevail in such cases where they impose more restrictive obligations than the IPPs. The Guidelines cannot, however, permit something that is otherwise prohibited by the IPPs.

A breach of the Guidelines constitutes an interference with privacy under section 13 of the Privacy Act. In turn, an individual may complain to the Privacy Commissioner about an alleged interference with their privacy.

### Significant changes from the previous guidelines

While the operation and effect of each guideline is described in the section below, it may be helpful to briefly describe the main changes between these Guidelines and those that they replace. Changes between the current and former instruments are generally a result of either of the following:

- Where permitted by the enabling legislation, the Privacy Commissioner has, in some places, exercised discretion to change the operation of the Guidelines in response to stakeholders' submissions during the review process; or

- in a number of places, changes have been made where it is felt that the previous guidelines may not have adequately satisfied the requirements of the enabling legislation, particularly in regard to matters about which the Privacy Commissioner has no discretion.

In addition, in some places, changes have been made to promote clarity in how the Guidelines are presented.

Significant changes between these and the previous Guidelines include:

- The introduction of a new guideline prohibiting any Australian Government agency from combining information obtained from the Medicare Benefits or Pharmaceutical Benefits programs on the one database (see Guideline 1). The making of a guideline to this effect is an express requirement of section 135AA(5)(d) of the enabling legislation.

- The period for which linked datasets may be retained by Medicare Australia has been varied from a prescribed period (three months) to a principle-based approach whereby the datasets may be retained for as long as is reasonably necessary to meet the purpose for which they were created. The Privacy Commissioner is satisfied that such a measure, when accompanied by new reporting obligations (discussed below) provides an appropriate balance between the needs of the agency and the protection of individuals' privacy.

- Medicare Australia must annually report to the Privacy Commissioner on how many records from each program are linked, under what authority they are linked, how many of these linked datasets were destroyed in the period or why they were not destroyed. These reports will be publicly available.

- Medicare Australia is no longer required to delete claims information once it becomes 'old information' (that is, after five

years from when it was collected). Over time, this is intended to remove a significant administrative burden created by the need to obtain such old information, under certain permitted circumstances, from the Department. However, Medicare Australia must remove personal identifiers from that information after five years, and may only re-identify the information in certain limited circumstances.

- Medicare Australia must annually report to the Privacy Commissioner on how many records of 'old information' are linked to their identifying details, as well as the authority under which they are linked and information regarding the destruction of such linked datasets. These reports will be publicly available.

- The Secretary of the Department may delegate certain decisions to the level of First Assistant Secretary in that Department.

- The new Guidelines do not include an equivalent to the previous guideline 5.2(a),[2] which applied to the Department. The Privacy Commissioner formed the view that the previous guideline did not meet the statutory prohibition against combining claims information on the one database. This was discussed in detail in the Office's Review Report on the previous guidelines.[3]

# 4. SPECIFIC OPERATION

### Part A of the Guidelines – Australian Government Agencies

This part applies to all Australian Government agencies. The meaning of 'agencies' is as defined in section 6 of the Privacy Act. Part A includes one guideline only.

#### Guideline 1

Guideline 1 gives effect to section 135AA(5)(d), which requires an absolute prohibition against agencies storing claims information on the one database.

Section 135AA of the National Health Act requires the Privacy Commissioner to issue guidelines that, as far as practicable, regulate the handling of claims information by agencies. The Privacy Commissioner is satisfied that the term "so far as practicable" refers to the feasibility of using the Guidelines to achieve the objectives set out by the legislation, rather than what "is practicable" for any party affected by the Guidelines. For example, it may not

[2] This previous guideline provided that:

> 5.2 The Secretary must not permit the establishment of a system which maintains the de-identified records from both programs in a combined form on a permanent basis in conjunction with the internal personal identification number.
>
> (a) Nothing in this Guideline prevents the retention of de-identified records from both programs in a combined form in conjunction with an encrypted form of the internal personal identification number or a new and unrelated number.

[3] This is discussed specifically at p 68 of the Review Report, available at http://www.privacy.gov.au/act/review/healthreview.html#mozTocId523459.

be practicable to draft guidelines that prescriptively regulate the minutiae of various processes that occur when claims information is linked.

In regard to Guideline 1, it is practicable for the Guideline to give effect to the clear and express requirement of section 135AA(5)(d). Further, as the provision is drafted without allowance for any exceptions, there would appear to be no discretion to alter the requirement that claims information be kept on separate databases when held by Australian Government agencies.

While the primary record holders of claims information are Medicare Australia and the Department, Guideline 1 prescribes the general obligations which all agencies[4] must meet.

The extension of this prohibition to all agencies ensures that the Guidelines meet the statutory requirements of section 135AA(5)(d). The Privacy Commissioner has no discretion in making this guideline.

### Part B of the Guidelines – Medicare Australia

Parts B and C of the Guidelines apply to the two agencies that will most commonly handle claims information, these being Medicare Australia and the Department, respectively, while Part D provides miscellaneous guidelines which apply to both of these agencies.

Part B applies specifically to Medicare Australia and imposes certain obligations as to how that agency may handle claims information. These obligations are codified in Guidelines 2-6.

#### Guideline 2

Other than the option to publish technical standards reports provided by Medicare Australia to the Privacy Commissioner (see Guideline 2.5), Guideline 2 broadly reflects previous obligations imposed on that agency.

Guidelines 2.1 and 2.2 respectively provide for the separation of claims information in different databases, and the separation of those databases from enrolment and entitlement databases.

Guideline 2.3 ensures that claims information in the Medicare Benefits Program and Pharmaceutical Benefits Program databases are stripped of personal identification components,[5] such as name and address information, with the exception of a Medicare card number, or a Pharmaceutical entitlements number.

Information that is more than five years old is considered “old information”, and this information must not be stored with any personal identifying components, including the Medicare card number or the Pharmaceutical entitlements number. This is reflected in Guideline 5.1(b).

[4] Excluding those Australian Government agencies not regulated by the Privacy Act – see, section 135AA(11) of the *National Health Act 1953* (Cth).

[5] “Personal identification components” is defined in s 135AA(11) of the *National Health Act 1953* (Cth) as including a person’s name and address, their Medicare Card Number and their Pharmaceutical entitlements number.

Guideline 2.4 requires that Medicare Australia must establish standards to ensure a range of technical matters are adequately dealt with in designing a computer system to store claims information. These standards include ensuring adequate security arrangements as required in Guidelines 4.2 and 5.4, and measures to restrict access to the relevant databases; restricting the linkage of information held on the relevant databases, and the means to trace those linkages; and specifying destruction schedules for linked information.

These technical standards, and any variations thereof, must be provided in a report to the Privacy Commissioner. The Technical Standards Report must be lodged with the Commissioner within six months of the date that the Guidelines come into effect (subject to section 135AA of the National Health Act, the Guidelines' date of effect is 1 July 2008).

The Privacy Commissioner may, in consultation with Medicare Australia, make the technical standard reports publicly available as stated in Guideline 2.5. Such availability would not occur where it may not be in the public interest, such as where details in the reports may reveal security measures adopted by Medicare Australia to protect claims information, or where it may reveal processes relating to investigations.

This Guideline also incorporates provisions on the creation of a Medicare Australia personal identification number ('Medicare Australia PIN') that is unique for each individual, and the purposes for which a Medicare Australia PIN may be used or disclosed. It is the intent of the Guidelines that any such unique number be kept, as far as possible, within Medicare Australia and not used as an identifier for other purposes.

Guideline 2.7 limits the extent to which a Medicare Australia PIN can be used to identify individuals making claims under the Medicare Benefits Program or the Pharmaceutical Benefits Program.

## Guideline 3

Guideline 3 gives effect to section 135AA(5)(e) of the National Health Act, which requires guidelines be made prohibiting the linkage of claims information except in authorised circumstances.

In brief, the purposes for which Medicare Australia may link claims information are limited to where the linkage:

- is necessary to enforce a law;
- is required by law;
- is for the protection of the public revenue;
- is necessary to determine an individual's eligibility for benefits; or
- is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

Most significantly, in response to submissions from a range of stakeholders, a new authorised linkage has been added that was not in the previous guidelines. This allows claims information from the two claims databases, about the same individual, to be linked for the purpose of disclosing that claims information to the individual where the individual has consented. This

addition was made to permit individuals to receive, at their request, a single report of their Medicare Benefits and Pharmaceutical Benefits programs claims histories. It is codified in Guideline 3.1(e).

While someone acting on an individual's behalf with appropriate lawful authority may also consent to linkage in these circumstances, the Guideline authorises disclosure of the information to the individual themselves. This provision is not intended to be a consent mechanism to link claims information for unspecified secondary uses.

### Guideline 4

Previously, Medicare Australia had been limited in the duration for which it could retain linked claims information to three months, or until certain ongoing matters had been resolved (such as investigations, prosecutions, compensation matters or action for recovery of debt, or where the information affects an individuals entitlement to a related service which could be rendered after the expiry of the time limit).

Guideline 4 varies this obligation by requiring Medicare Australia to delete all linked datasets when the purpose for their linkage has been met. In some instances, this will have the effect of requiring Medicare Australia to destroy linked datasets almost immediately.

Equally, there will be linkages which need to be retained for longer periods than were previously allowed, however strict attention to identification of the purpose for which the information is linked will minimise the privacy risks of retaining linked information.

Guideline 4 requires Medicare Australia to make special arrangements for the security of linked claims information, and report these to the Privacy Commissioner (as discussed above at Guideline 2).

Guideline 4.1 requires information linked in accordance with Guideline 3.1 to be destroyed as soon as practicable after the purpose of the linkage has been met.

The practicability of destruction may be determined in part by reference to the destruction schedules specified in Guideline 2.4(f). For example, where claims information is linked for the purpose of providing a consolidated claims history to an individual, the purpose of that linkage is effectively met at the moment the disclosure occurs. It may not be practicable for that linked dataset to be destroyed instantaneously, though it may be practicable for its destruction to be effected within a defined destruction cycle of a few days.

Any destruction schedule would only be applicable to the extent that it is consistent with the intent of the enabling legislation and Guidelines. In the above example, it would be unlikely to be appropriate for such datasets to only be deleted as part of a cycle that occurs every few months.

As a form of additional oversight, Guideline 4 introduces reporting requirements, under which Medicare Australia will be required to submit annual reports to the Privacy Commissioner on how it has handled linked claims information.

Such reports must include, for the relevant reporting period:

a) the number of records linked;

b) the number of records linked under each of the permitted circumstances of Guideline 3.1;

c) the number of linked records that were destroyed;

d) the number of records destroyed that were linked under each of the permitted circumstances of Guideline 3.1;

e) reasons for the retention of any linked records that were not destroyed during the reporting period; and

f) the total number of records linked in accordance with Guideline 3.1 that have been retained from previous reporting periods, and reasons for their retention.

The reporting obligations referred to in a) and b) are intended to provide oversight of data linkage activities by requiring information on how many datasets were created and for what purpose. Reporting obligations c) to f) are intended to provide the Privacy Commissioner with an indication as to whether linked datasets are being retained for periods of time that may be longer than envisaged, and if so, why.

In particular, if the number of datasets reported under obligation d) were to be significant, it could indicate that these datasets were being retained for periods that are inconsistent with the policy intent of the enabling legislation. In such circumstances, it be would open for the Privacy Commissioner to make further enquiries of Medicare Australia (including, where necessary, by exercising formal audit powers).

These reporting obligations reflect the intent envisaged when the Office released its Review Report on the previous Guidelines, and have been developed in consultation with Medicare Australia. They are intended to promote transparency in how claims information is linked.

## Guideline 5

Section 135AA(5)(f) requires that the Privacy Commissioner make guidelines concerning the handling of 'old information'.[6] 'Old information' is defined as claims information that has been held by one or more agencies for more than

[6] The provision says, in full:
(5) So far as practicable, the guidelines must:
...
(f) specify the requirements with which agencies must comply in relation to old information, in particular requirements that:
(i) require the information to be stored in such a way that the personal identification components of the information are not linked with the rest of the information; and
(ii) provide for the longer term storage and retrieval of the information; and
(iii) specify the circumstances in which, and the conditions subject to which, the personal identification components of the information may later be re-linked with the rest of the information.

five years. It particularly requires that this old information be stored without its 'personal identification components'.

Guideline 5 amends the previous arrangements by which Medicare Australia may handle old information.

Previous Guideline 3.1 required that Medicare Australia must delete all claims information within five years of its initial processing. In certain limited circumstances, Medicare Australia was able to retrieve claims that it provides on a routine basis to the Department.

The Privacy Commissioner has accepted that the number of occasions where Medicare Australia may validly retrieve old information from the Department has increased significantly. This had created a regulatory and administrative burden for both agencies. The new Guidelines will help alleviate this burden while maintaining appropriate privacy protections for the storage of claims information and linked datasets by Medicare Australia.

Under Guideline 5, Medicare Australia will no longer be required to delete claims information within five years. Medicare Australia will be able to retain claims information indefinitely, but must strip such claims information of its identifying components after five years. Medicare Australia may only re-link this old information to its personal identifying components for a limited range of prescribed purposes under Guideline 5.2. The re-linkage is facilitated by the Medicare Australia PIN.

Once the purpose for which the old information has been linked with its personal identifying components is fulfilled, the linked dataset must be destroyed as soon as practicable. As with linked claims information in Guideline 4.1, what is a "practicable" period within which datasets must be deleted may be determined in part by reference to the destruction schedule specified in Guideline 2.4(f) (although such determination is not bound by this).

Medicare Australia must make special arrangements for the security of linked old information, and report these to the Privacy Commissioner (as discussed above at Guideline 2).

Guideline 5.5 introduces reporting obligations on Medicare Australia under which it must report annually to the Privacy Commissioner on how it has handled old information.

Such reports must include details similar to those required for the linkage of claims information that is not old information (detailed above under Guideline 4) and will be made publicly available.

Guideline 5.7 permits the transfer of old information from the Department to Medicare Australia for two reasons: for a purpose listed under Guideline 5.2 and for inclusion into its databases of old information described in Guideline 5.1. In some ways Guideline 5.7 can be seen as a transitional guideline, because Medicare Australia will not collect all old information stored by the Department immediately. This Guideline provides a mechanism for old information to be collected progressively by Medicare Australia, though such information must be stored on a different database to personal identification components.

## Guideline 6

Guideline 6 permits Medicare Australia to disclose claims information to researchers for the purpose of medical research in certain circumstances. Claims information that identifies an individual may only be disclosed with that individual's consent or in compliance with the guidelines issued by the National Health and Medical Research Council (NHMRC) under section 95 of the Privacy Act.

These arrangements reflect obligations that would apply under the Privacy Act and related laws regardless of whether this Guideline is made. However, the Privacy Commissioner is satisfied that the inclusion of this Guideline clarifies and provides certainty regarding how claims information may be used for medical research purposes.

Guideline 6.2 varies the requirement under previous Guideline 4A.2 which purported to impose an obligation on a researcher to whom claims information was disclosed.[7] However, the Privacy Commissioner has noted that the application of the Guidelines is limited to Australian Government agencies, and accordingly it was beyond the authority of the Guidelines to purport to impose obligations on researchers outside of the Australian Government.

Accordingly, the new Guideline 6.2 places the obligation on Medicare Australia, as the regulated party, to obtain agreement from the researcher regarding the secure destruction of the records at the conclusion of the research project.

### Part C of the Guidelines – Australian Government Department of Health Ageing

This part applies specifically to the Department and imposes certain obligations as to how the Department may handle claims information. These obligations are codified in Guidelines 7 and 8.

## Guideline 7

Guideline 7 amends the previous Guideline 5, and relates to the use of claims information by the Department. Significantly, this Guideline, and Guideline 8, now allow the Secretary of the Department to delegate some decision making powers to the level of First Assistant Secretary (see the definition of "delegate" under "Meaning of terms" in the Guidelines).

The Department may only use the claims information as authorised by the Secretary of the Department or their delegate. In a requirement reflecting the obligations on Medicare Australia, the Department must not store claims information from both programs in a combined form on a permanent basis.

Claims information may be held by the Department indefinitely for policy and research purposes in a form that does not include personal identification components. However, where the information is linked by the Medicare Australia PIN, there are restrictions. The Department may link the information, using the Medicare Australia PIN:

[7] This obligation required researchers to return or delete claims information when the research was concluded.

- where it is necessary for an authorised use; and
- where the identified information is used solely as a necessary intermediate step to obtain aggregated data or otherwise de-identified information; and
- only where there is no practical alternative.

Any claims information linked to its personal identification components must be destroyed within one month of its linkage.

The Department must not disclose claims information unless it is reasonably satisfied that the recipient will not be able to identify the individual to whom it relates, unless it is to Medicare Australia, or the information is released under the secrecy provisions of section 130 of the *Health Insurance Act 1973* or section 135A of the *National Health Act 1953*.

### Guideline 8

There are circumstances in which it may be necessary for the Department to have access to identified claims information. Guideline 8 allows the Department to obtain the personal identification components that belong to a particular Medicare Australia PIN from Medicare Australia in certain limited circumstances. The Department may link claims information to the individual's name where authorised by the Secretary of the Department, or delegate, for the purpose of clarification, where a doubt has arisen in relation to linking of de-identified information. However, procedures must ensure that identified information is not retained once the doubt has been resolved.

The Department may also re-identify information for a disclosure that is expressly authorised or required by law. The Department is required to maintain, and make publicly available, a policy statement regarding its usual practices where information is identified and disclosed in this way. It must also maintain, under strict security controls, a central record of those linkages.

The Secretary of the Department, or delegate, must establish procedures which ensure that a request for identified information is usually referred to Medicare Australia.

## Part D of the Guidelines – Medicare Australia and the Australian Government Department of Health Ageing

This part provides a range of miscellaneous matters which apply to both Medicare Australia and the Department.

### Guideline 9

This Guideline includes a range of provisions that apply to both Medicare Australia and the Department. The regulatory obligations are largely unchanged from the previous guidelines, in that they:

- prohibit the generation of a paper copy of a complete database or databases, or major proportions of those databases;
- require that the Privacy Commissioner be informed of any arrangements made between Medicare Australia and the

Department which relate to delegations or authorisations for implementing the Guidelines; and

- require Medicare Australia and the Department to educate staff regarding the privacy protections that apply to claims information.

To ensure clarity, Guideline 9.4 also provides that where a Guideline provides more restrictive regulation than the requirements in the Privacy Act (such as under the IPPs) or the secrecy provisions of relevant legislation as applying to Medicare Australia and the Department, the Guideline prevails.

# 5. CONSULTATION

Before issuing guidelines, the Privacy Commissioner is required under section 135AA(6) of the National Health Act to take reasonable steps to consult with organisations, including agencies, whose interests would be affected by those guidelines. Such consultation is also consistent with section 17 of the *Legislative Instruments Act 2003*.

This consultative process was undertaken as part of the Office's review of the previous guidelines during 2004 to 2006. In conducting this review, the Office noted that principles of good regulatory practice suggest that regulatory instruments should be reviewed at intervals of no more than 10 years. A number of other factors pointed to the timeliness for the review, including:

- developments in information technology which may have bearing on the handling of health information when stored electronically;
- suggestions that the information covered by the then Guidelines could be more usefully utilised by researchers than was currently the case;
- evidence of increasing use of information technology in the planning and provision of health services;
- suggestions that community attitudes and expectations regarding the handling of personal information, and in particular sensitive health information, may have changed since the Guidelines were introduced; and
- a request from the Department that the review be conducted in light of changes to the health environment.

## Consultation process

The Privacy Commissioner encouraged agencies, organisations and the general public to participate in the review of the previous guidelines in a number of ways, including:

- a media and web announcement[8] in November 2004
- advertisements placed in national and local papers, health sector journals and other publications including:

[8] http://www.privacy.gov.au/news/04_06.html

  - the Health ICT News/Health ICT Headlines email bulletin,11 November 2004
  - *Medical Observer,* 12 November 2004
  - the Australasian Epidemiological Association email bulletin,12 November 2004
  - the *Weekend Australian*, 13 November 2004
  - the *Privacy Law Bulletin*, 17 November 2004
  - the *Brisbane Courier Mail*, 18 November 2004, and
  - the *Northern Territory News*, 18 November 2004
- directly inviting potential stakeholders to make submissions.

### Issues Paper

To assist stakeholders in contributing to the review, the Privacy Commissioner released an Issues Paper on 8 November 2004.[9]

The Issues Paper raised a number of matters concerning the then Guidelines. These included the health environment, information linkage and secondary uses of health information, the retention of claims information, as well as issues surrounding consent and access, community attitudes and the ease of use of those guidelines.

The matters raised in the Issues Paper were not intended to be exhaustive, but were intended to encourage submissions on a broad range of issues which it was felt may help to inform the Office's considerations.

### Open forums

The Office conducted a series of open forums in all states and territories except Western Australia.[10] Forums were held in 2004 in Brisbane (22 November), Darwin (25 November), Adelaide (29 November), Melbourne (7 December), Hobart (9 December), Canberra (14 December) and Sydney (15 December).

These forums were attended by representatives of the Australian, State and Territory governments, the private sector and individuals from the health sector, including general practitioners, researchers, consumer advocates and members of the public.

### Written submissions

The Privacy Commissioner received 35 written submissions to this review from a range of stakeholders, including peak health professional bodies, the Australian Privacy Foundation, Consumers' Health Forum of Australia, a number of pharmaceutical and health insurance companies, as well as government bodies, including Medicare Australia and the Department of Health and Ageing. Of these, three submitters requested that their names

[9] http://www.privacy.gov.au/health/guidelines/healthreview.html#c

[10] A meeting was scheduled for Perth, however this was cancelled due to insufficient confirmed attendees.

and or submission be treated confidentially. The remaining 32 submissions can be found on the Office's website.[11] These submissions were received by 4 February 2005.

### Consultative group

At the end of the public consultation process on the Issues Paper, the Privacy Commissioner formed a consultative group to assist in considering issues raised in the review. This group consisted of the:

- Australian Government Attorney-General's Department
- Australian Government Department of Health and Ageing
- Australian Institute of Health and Welfare
- Australian Medical Association
- Australian Privacy Foundation
- Health Consumer's Council (WA)
- Health Insurance Commission (now Medicare Australia) and
- Caroline Chisholm Centre for Health Ethics.

An Options Paper was provided to this group on 29 April 2005. This paper was subsequently discussed at a meeting in Sydney on 5 May 2005.

In finalising this report, the Office held additional meetings with Medicare Australia and the Department through 2005 and 2006.

### Further consultation

Following the release of the final report of the review in August 2006, and as envisaged in that report, throughout 2007 the Office had detailed discussions with Medicare Australia as well as the Department, to ensure the requirements in the proposed Guidelines were effective and appropriate.

[11] http://www.privacy.gov.au/health/guidelines/healthsubs.html

## ATTACHMENT A: SECTIONS 135AA AND 135AB, *NATIONAL HEALTH ACT 1953*

### 135AA Privacy guidelines

*Information to which this section applies*

(1) Subject to subsection (2), this section applies to information that:
  (a) is information relating to an individual; and
  (b) is held by an agency (whether or not the information was obtained by that agency or any other agency after the commencement of this section); and
  (c) was obtained by that agency or any other agency in connection with a claim for payment of a benefit under the Medicare Benefits Program or the Pharmaceutical Benefits Program.

*Information to which this section does not apply*

(2) This section does not apply to such information:
  (a) so far as it identifies:
    (i) a person who provided the service or goods in connection with which the claim for payment is made; or
    (ii) a person who, in his or her capacity as the provider of services, made a referral or request to another person to provide the service or goods; or
  (b) so far as it is contained in a database that:
    (i) is maintained for the purpose of identifying persons who are eligible to be paid benefits under the Medicare Benefits Program or the Pharmaceutical Benefits Program; and
    (ii) does not contain information relating to claims for payment of such benefits; or
  (c) so far as it is not stored in a database.

*Issuing guidelines*

(3) The Privacy Commissioner must, by written notice, issue guidelines relating to information to which this section applies.

*Replacing or varying guidelines*

(4) At any time, the Privacy Commissioner may, by written notice, issue further guidelines that vary the existing guidelines.

*Content of guidelines*

(5) So far as practicable, the guidelines must:
  (a) specify the ways in which information may be stored and, in particular, specify the circumstances in which creating copies of information in paper or similar form is prohibited; and
  (b) specify the uses to which agencies may put information; and
  (c) specify the circumstances in which agencies may disclose information; and
  (d) prohibit agencies from storing in the same database:
    (i) information that was obtained under the Medicare Benefits Program; and

(ii) information that was obtained under the Pharmaceutical Benefits Program; and

(e) prohibit linkage of:

(i) information that is held in a database maintained for the purposes of the Medicare Benefits Program; and

(ii) information that is held in a database maintained for the purposes of the Pharmaceutical Benefits Program;

unless the linkage is authorised in the way specified in the guidelines; and

(f) specify the requirements with which agencies must comply in relation to old information, in particular requirements that:

(i) require the information to be stored in such a way that the personal identification components of the information are not linked with the rest of the information; and

(ii) provide for the longer term storage and retrieval of the information; and

(iii) specify the circumstances in which, and the conditions subject to which, the personal identification components of the information may later be re-linked with the rest of the information.

(5A) Nothing in this section, or in the guidelines issued by the Privacy Commissioner, precludes the inclusion, in a database of information held by the Medicare Australia CEO and relating to claims for benefits under the Pharmaceutical Benefits Program, of the pharmaceutical entitlements number applicable to the person to whom each such claim relates:

(a) as a person covered by a benefit entitlement card; or

(b) as a person included within a class identified by the Minister in a determination under subsection 86E(1).

*Consultation*

(6) Before issuing guidelines, the Privacy Commissioner must take reasonable steps to consult with organisations (including agencies) whose interests would be affected by the guidelines.

*Disallowance*

(7) Guidelines are disallowable instruments for the purposes of section 46A of the *Acts Interpretation Act 1901*.

*When guidelines take effect*

(8) Despite section 46A and paragraph 48(1)(b) of the *Acts Interpretation Act 1901*, guidelines take effect from:

(a) the first day on which they are no longer liable to be disallowed; or

(b) if the guidelines provide for their commencement after that day—in accordance with that provision.

*Failure to table first guidelines within 6 months*

(9) If guidelines issued under subsection (1) are not laid before each House of the Parliament under paragraph 48(1)(c) of the *Acts Interpretation Act 1901* (as applied by section 46A of that Act) within 6 months after the commencement of this section, the Privacy Commissioner must report the failure to issue guidelines

within that period to each House of the Parliament within 15 sitting days of that House after the end of the period.

*Tabling first guidelines after 6 months*

(10) Subsection (9) does not render invalid guidelines issued under subsection (3) that are not laid before each House of the Parliament within that period.

*Definitions*

(11) In this section:

***agency*** has the same meaning as in the *Privacy Act 1988*.

***benefit entitlement card*** means:

(a) a medicare card within the meaning of subsection 84(1); and

(b) a card that evidences the person's status as a concessional beneficiary within the meaning of subsection 84(1).

***database*** means a discrete body of information stored by means of a computer.

***Medicare Benefits Program*** means the program for providing Medicare benefits under the *Health Insurance Act 1973*.

***old information*** means information to which this section applies that has been held by one or more agencies for at least the preceding 5 years.

***personal identification components***, in relation to information, means so much of the information as includes any of the following:

(a) the name of the person to whom the information relates;

(b) the person's address;

(c) the person's Medicare card number;

(d) the person's Pharmaceutical entitlements number.

***Pharmaceutical Benefits Program*** means the program for supplying pharmaceutical benefits and special pharmaceutical products under Part VII of this Act.

***pharmaceutical entitlements number***, in relation to a person, means:

(a) if the person is covered by a medicare card—a medicare number within the meaning of subsection 84(1) that is applicable to the person as a person covered by that card; and

(b) if the person is covered by a card that evidences the person's status as a concessional beneficiary within the meaning of subsection 84(1)—the number applicable to that person as a person covered by that card.

## 135AB Breaches of the privacy guidelines

(1) A breach of the guidelines issued under section 135AA constitutes an act or practice involving interference with the privacy of an individual for the purposes of section 13 of the *Privacy Act 1988*.

(2) An individual may complain to the Privacy Commissioner about an act or practice in relation to the operation of guidelines issued under section 135AA of this Act which may be an interference with the privacy of an individual.

(3) If a complaint is made, Part V of the *Privacy Act 1988* applies, with such modifications as the circumstances require, as if the complaint were an IPP complaint (within the meaning of that Act) made under section 36 of that Act.