Information Management

KCS Policy

CONTENTS

COMMUNICATION STRATEGIES

Underpinning the management of information in Kogarah Community Services are the following communication strategies:

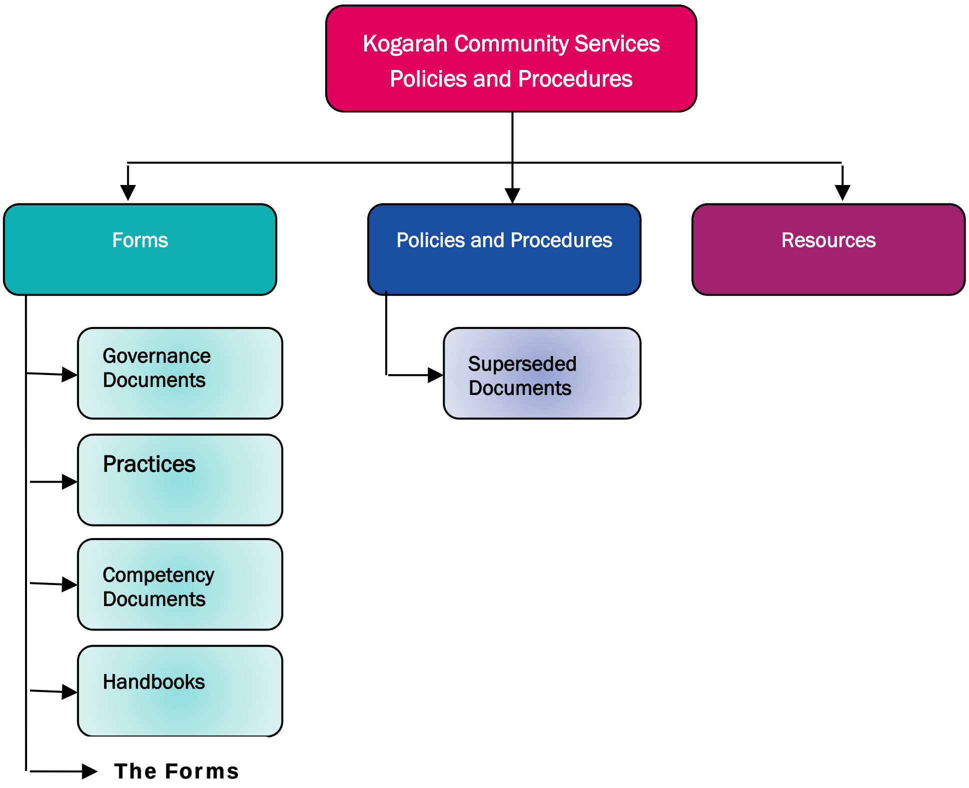
- Regular and structured meetings that involve all staff (see KCSP007 8.3.2 Governance Processes/ Management meetings)
- Regular reporting (see KCSP007 8.3.4 Performance Reports)
- Training for staff in relevant policies and procedures
- Involvement of staff and consumers in the Continuous Improvement process (see KCSP014 Continuous Improvement)
- Involvement of staff in the planning process (see ACP602 Planning)
- A newsletter for staff and consumers prepared by the relevant team members
- Emails and memos to staff as required
- Letters and notices to consumers as required.

POLICIES AND PROCEDURES

Structure of the policies and procedures

Our policies and procedures include the components shown in Figure 8.11.1: Policies and Procedures Schema.

Figure 8.11.1: Policies and Procedures Schema



The policies and procedures are maintained as read-only documents in the policies and procedures folder on the intranet. The CEO is responsible for ensuring the information is up-to-date with assistance from the management team and other staff as required. The involvement of all staff is encouraged to ensure policies and procedures reflect practice and to foster ownership and familiarity with the material.

The policies and procedures include the following sections:

Aged Care Quality Standards:
1. Consumer Dignity and Choice
2. Ongoing Assessment and Planning
3. Personal Care and Clinical Care
4. Services and Supports for Daily Living
5. Service Environment
6. Feedback and Complaints
7. Human Resources
8. Organisational Governance

Children's Services Quality Standards:
1. Educational Program and Practice
2. Children's Health & Safety
3. Physical Environment
4. Staffing Arrangements
5. Relationships with Children
6. Collaborative Partnerships with Families & Communities
7. Leadership & Service Management

Forms

A copy of each form used by Kogarah Community Services is maintained in the staff intranet in the subfolder Forms and is referred to in the policies and procedures.

Access to policies and procedures

All staff can access the policies and procedures either through their own computer terminal or through the shared terminals available in the KCS office. If staff require a paper copy of procedures these can be requested from their manager. (see 8.11.2 policies and procedures/control of the policies and procedures).

Updating the policies and procedures

The need to update the policies and procedures, forms or other material may occur through:

- Changes in legislation or regulations
- Changes in funding or funding guidelines and requirements
- Feedback
- Management decisions
- Adverse Event Reports
- Audits and
- Reviews.

The process for updating the policies and procedures, forms etc. is:

- When the need for changes is identified these are discussed with the relevant Program Manager.
- The Program Manager delegates an appropriate person/s to draft changes.
- Draft changes are reviewed by the Program Manager:

  - If the changes relate to a policy and procedures or practice, these are submitted to the Clinical Care Committee (clinical) or Improvement Committee (corporate). Once the Clinical Care Committee has approved the change, the Improvement Committee endorses the change. A list of all Improvement Committee endorsed policy and procedures and practice documents is provided to the Leadership Team meeting for noting.
  - The Program Manager may approve forms and other document changes.
- When changes have been approved by Improvement Committee and noted by the Leadership Meeting the Administration team is advised to update the policies and procedures and relevant documents.
- The policy and procedures are updated including forms and the table of contents. Old versions are archived.
- Note that any new form is referenced in the policies and procedures.
- Staff are advised of changes to the policies and procedures either through a staff meeting, an email, a memo or a training session. Consumers are advised, as appropriate and necessary, through staff, the newsletters, email or handbook or flyers.
- Major changes to the policies and procedures are recorded as an improvement in the Plan for Continuous Improvement (see KCSP014 Continuous Improvement).
- Major changes are reviewed after an appropriate time to ensure they have achieved the required outcome.

Review minutes of management meetings

A delegated staff member reviews the minutes of all staff and management meetings for decisions that need to be reflected in the policies and procedures.

Control of the policies and procedures

- Electronic read-only copies of the policies and procedures material are accessible to staff
- Only the CEO and management team can initiate changes to the original files and only within the specified process (see 8.11.2 policies and procedures/ updating the policies and procedures).
- Printed pages of the policies and procedures can be made for staff to refer to but are uncontrolled documents once printed (other than the authorised printed copy/copies). These must be kept to a minimum. The Office Manager is responsible for recording the location of any full copies of the policies and procedures and for ensuring that they are updated when the originals are updated.

Review of policies and procedures

Policies and procedures including forms are reviewed over a three-year period as documented in the Corporate Calendar. This is described in detail in 8.9 Continuous Improvement.

CONSUMER INFORMATION

Principles for the collection of consumer information

(See ACP103 1.3.6 Consumer Rights and Responsibilities/Consumer rights/Personal information.)

Management of consumer information

The Aged Care Act[1] specifies the kinds of records that must be kept by aged care providers. These include:

[1] Sections 63-1(1)(a) and 87-2 of the Aged Care Act 1997 and Part 7B of the Aged Care Quality and Safety Commission Act 2018 cited in Australian Government Department of Health and Aged Care Home Care Packages Program Operational Manual A Guide for Home Care Providers Version 1.1 – February 2021 Appendix D: Responsibilities of approved providers Accountability – Part 4.3 in the Aged Care Act 1997p 127 (Click on link for latest version) This information can be applied to all programs

- Assessments of consumers
- Individual support/care plans
- Medical records, progress notes and other clinical records
- Schedules of fees and charges
- Agreements
- Accounts of consumers
- Records relating to consumers' entry, discharge and leave arrangements, including death certificates where appropriate
- Records relating to a determination that a consumer is a consumer with financial hardship
- In relation to a continuing home care consumer to whom we start to provide home care through a home care service on or after 1 July 2014—a record of whether the consumer made a written choice regarding whether they would be covered by the pre or post-1 July 2014 arrangements
- UpToDate records of: the name and contact details of at least one representative of each consumer; and the name and contact details of any other representative of a consumer;
- Copies of unspent funds notices
- Records relating to the payment of the consumer portion or transfer portion of consumers' unspent home care amounts
- Copies of notices of published exit amounts
- Records required to be kept by the National Aged Care Mandatory Quality Indicator Program Manual.

Records are required to be kept for three years after the 30 June of the year in which we cease to provide care to the consumer.

(See also 8.11.6 Archiving/Table 8.11.1 Timelines for Maintaining Records)

Paper records

Generally, all consumer information is recorded on the Consumer Management System, however a paper file is required for some documentation.
(See ACP206 Consumer Documentation and Information Sharing.)

Office Files

Office files are created as required by the Administration Team and stored in lockable filing cabinets. the Administration Team are also responsible for filing and for securing the files.

In-home Files

ACS Consumers who have in-home services also have a home file that includes information required by Support Workers. (See ACP206 2.6.2 Access to Support Plans and Other Documentation/Home care file contents).

Electronic Records

Consumer information is also stored electronically on Consumer Management Systems. The Administration Teams are responsible for ensuring that data entry is completed (including entering a new consumer, amending data, exiting consumers, setting up invoices and rostering workers).

Aged Care - Staff record all consumer services and case notes in the Consumer Management System as well as in the consumer's home notes as necessary. Financial records for Home Care Package Consumers including an individualised budget are maintained for each HCP consumer on the Consumer Management System.

Information is restricted by passwords to relevant staff. Information systems for the effective documentation and communication of support planning are described in Section 2: Assessment and Planning (see ACP203 2.3.6 Assessment and Support Planning Process/Service Commencement Meeting and ACP203 2.3.7 Support Plans).

Consumer access to information

(See KCSP026 1.6.3 Consumers Right to Access Information.)

RECORDING SERVICE DELIVERY INFORMATION

Information on the support services delivered to consumers is recorded on the Consumer Management System. The Administration Team are responsible for the entry of information and for the preparation of reports as outlined in KCSP007 8.3.4 Performance Reports.

GENERAL INFORMATION

The Administration Team are responsible for organising and maintaining the filing of general information and keeping it up to date.

Staff records

Staff files are held electronically within Employment Hero, our online HR platform. The CEO and Program Managers can access and manage their staff files through this platform.

Staff access to staff files

(See KCSP020 7.3.9 Staff Files.)

Minutes of meetings

Minutes of meetings are maintained on the shared drive.

Other administrative information

All other administrative information including funding information, financial information and general filing is maintained on the shared drive.

ARCHIVING

Archive management

The Administration Team is responsible for archive management. Archives are stored electronically, sorted by year and include::

- Consumer records
- Staff records
- Administrative records including financial records
- Policies and procedures.

Aged care act responsibilities[2]

We ensure that we keep records (in written or electronic form) that enable proper assessments to be made of whether we have complied, or are complying, with our responsibilities under the Act. These records are required to be kept for a minimum of three years after the 30 June of the year in which the record was made. We keep the records for seven years.

Timelines for maintaining records

Records are securely destroyed after the time periods shown in Table 8.11.1 Timelines for Maintaining Records

Table 8.11.1 Timelines for Maintaining Records

Employment applications unsuccessful	6 months
Staff records	7 years after the staff person ceases employment
Consumer records	7 years after the consumer ceases receiving services
Financial records including claims for payments	7 years
Records relating to compliance with program requirements	7 years
General administrative records	7 years
Policies and procedures	7 years

Archiving consumer records

Consumer records are destroyed as per specified timelines (see Table 8.11.1 Timelines for Maintaining Records).

Consumer management system records

Exited consumers are de-activated on the Consumer Management System and re-activated if they return to the service (see Table 8.11.1 Timelines for Maintaining Records).

Managing superseded policies and procedures

Whenever changes are to be made to the policies and procedures or a form the following procedure applies:

- Before making changes copy the existing file into the Archived folder in Document Control
- Watermark the document 'Superseded'
- Add 'today's date' to the end of the file name – e.g. Corporate Governance 03/03/2011
- You can now make your changes to the original document.

Superseded policies and procedures and forms are destroyed as per the timelines specified in Table 8.11.1 Timelines for Maintaining Records.

[2] Australian Government Department of Health and Aged Care Home Care Packages Program Operational Manual A Guide for Home Care Providers Version 1.1 – February 2021 Appendix D: Responsibilities of approved providers Accountability – Part 4.3 in the Aged Care Act 1997 Record keeping p 127 (Click on link for latest version). This information can be applied to all programs

INFORMATION TECHNOLOGY AND CYBER SECURITY[3]

Our information technology systems ensure we can meet the needs of Kogarah Community Services, ensure the protection of consumer, staff and organisation information and support the collection of service delivery data and reporting obligations outlined in our Grant Agreements.

Cyber security

Strategies to ensure the safety of Kogarah Community Services data include:

- We only utilise cloud storage physically based in Australia (data sovereignty).
- Cameras, alarms and other Internet-of-Things devices are not connected to our data server.
- We utilise a Unified Threat Management firewall (UTM)
- All computers are password protected and set to lock after 30 minutes of non-use to prevent unauthorised access.
- We employ a user access policy where users are only granted access to data that they need to do their job. Access to data is further restricted by the assignment of usage levels including administrator, user and read only.
- Service delivery staff only have access to the data of consumers they are working with or likely to work with. Access is limited to information directly related to their work such as the support plan and notes.
- A backup cycle to removable disk, with an off-site copy, is maintained as another level of safety in the event of data loss on the server.
- All server equipment is maintained in a secure room that is locked when physical access to equipment is not required.
- A mobile device manager is utilised to manage all access to our data by staff using mobile phones/devices. This includes remote wipe and remote delete functions for use in the event of loss of the device.
- Complex passwords are created randomly by the system administrators only and are changed yearly or whenever a staff person leaves Kogarah Community Services. Under no circumstances are staff permitted to disclose their password to any other person.
- Two factor authentication is utilised wherever feasible
- Only the IT and Data Support Coordinator or designated system administrators can add new data folders to the shared drive of the server.
- An anti-virus program including anti anti-ransom-ware is maintained on every device connected to the server.
- No programs, external data or utilities can be installed onto any workstation or other device without the permission of the system administrators.
- All systems software is maintained up to date.
- Our IT Consultant reviews our system and our data breach procedures at least annually and whenever a data breach related to IT occurs
- All staff receive information on our IT system requirements and training on responding to data breaches on commencement with the service.

Email

Staff may send and receive minimal personal emails.

[3] Please note: This Section will vary greatly depending on the size of your organisation. The processes will be much simpler for smaller organisations. We recommend all providers consult with their IT specialist in customising this Section

All emails are filed in the appropriate folders set up by the system administrators. Emails documenting service feedback and information relevant to the operation of Kogarah Community Services are forwarded to the relevant staff person.

Internet access

Internet access is restricted to work related purposes and is monitored and audited.

MyGovID

MyGovID is required for access to the My Aged Care portal. The Coordinators and ACS administrative team are authorised to access My Aged Care, on behalf of Kogarah Community Services. The CEO is the Relationship Authorisation Administrator and authorises each individuals access to the portal.

Getting help and reporting problems

If a staff person experiences any problems with a program or computer or other piece of equipment, they can in the first instance contact the Office Manager. If necessary, the Office Manager arranges for IT Support to assist.

Social media

We are aware that social media (social networking sites (Facebook, Twitter etc.), video and photo sharing sites, blogs, forums, discussion boards and websites) promote communication and information sharing. Staff who work in Kogarah Community Services are required to ensure the privacy and confidentiality of the organisation's information and the privacy and confidentiality of consumer information and must not access inappropriate information or share any information related to their work through social media sites.

Staff are required to seek clarification from their manager if in doubt about what is information related to their work.

Consumer consent is required before any photographs, names or other information are published to social media.

Responding to data breaches

Data breach

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost. Data breaches include:

- Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- Unauthorised access to personal information by an employee
- Inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures. [4]

Notifiable data breaches

Under the Notifiable Data Breaches (NDB) scheme Kogarah Community Services is required to notify any individual whose data is breached and the Australian Information Commissioner of data breaches where:

[4] Australian Government Office of the Australian Information Commissioner Data Breach Preparation and Response (A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 (Cth) p 8

- There is unauthorised access to or disclosure of personal information held by Kogarah Community Services (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- Kogarah Community Services has been unable to prevent the likely risk of serious harm with remedial action.

(See Figure: 8.11.2: OAIC Data Breach Action Plan for Health Service Providers)[5]

Kogarah Community Services also reports the breach, when it is relevant to do so, to other organisations such as:

- Police or law enforcement bodies
- The Australian Securities & Investments Commission (ASIC)
- The Australian Prudential Regulation Authority (APRA)
- The Australian Taxation Office (ATO)
- The Australian Transaction Reports and Analysis Centre (AUSTRAC)
- The Australian Cyber Security Centre (ACSC)
- The Australian Digital Health Agency (ADHA)
- The Department of Health and Aged Care
- State or Territory Privacy and Information Commissioners
- Professional associations and regulatory bodies
- Insurance providers.

(See also KCSP026 1.6 Privacy and Confidentiality for details of how Kogarah Community Services respects consumer's privacy.)

Data Breach Response Plan

Key Roles

- Board of Management
  - Responsible for ensuring the security of Kogarah Community Services data
  - Are advised of all data breaches and actions taken to resolve and to prevent future breaches
  - Approve the procedures for security of data and responding to data breaches.
- Staff
  - All staff are responsible for minimising the chances of a data breach occurring
  - Staff are required to take particular care of any documents or devices, such as phones or laptops, that connect to or contain information related to consumers or Kogarah Community Services
  - In the event that a device or document is lost it must be reported immediately or as soon as it is known to be lost, to your manager
  - In the event of, or threat of (phishing or a virus) unlawful access to data on the computer system the IT Consultant is advised immediately, the system is immediately isolated and our computer consultant is requested to deal with the access or threat, identify the extent of the breach, how it occurred and how to prevent it in the future.

[5] Australian Government Office of the Australian Information Commissioner Action plan for health service providers 11 February 2020

- IT Consultant
  - Receives reports of data breaches
  - Takes any immediate necessary action to contain or resolve the breach
  - Investigates the breach if appropriate
  - Refers the breach to the CEO.
- Leadership Team
  - Action significant data breaches as reported by our IT Consultant
  - Review all data breaches
  - Review any immediate action taken
  - Identify and implement additional action required
  - Determine if the breach must be reported to the Commissioner under the Notifiable Data Breaches (NDB) scheme
  - Determine if it is likely that any person's data is at risk of being viewed or utilised by others and advise the affected persons
  - Ensure the protection of data is part of KCS' continuous improvement priorities
  - Testing of the data breach response plan.

Data Breach Report

Data breaches are reported using an Adverse Event Report with a Data Breach Report attached.

Procedure for Dealing with a Data Breach

In the event of a data breach or suspected breach the steps below apply as appropriate to the breach and to Figure: 8.11.2: OAIC Data Breach Action Plan for Health Service Providers.

- Immediately advise your manager of the breach and complete an Adverse Event Report with an attached Data Breach Report.
- The manager will determine if any immediate action can be taken to contain or resolve the data breach in consultation with the CEO (e.g. delete mobile phone, advise Police) and implement this action. The Adverse Event Report is updated.
- The manager advises our IT Consultant of the breach and of any action taken. The Adverse Event Report is updated.
- The IT Consultant considers whether any other immediate action should be taken, including whether the breach must be reported to the Leadership Team to action. This is determined on:
  - The number of people affected by the breach or suspected breach
  - Whether there is a risk of serious harm to affected individuals now or in the future
  - Whether the data breach or suspected data breach may indicate a systemic problem with our practices or procedures
  - Other issues relevant to the circumstances, such as the value of the data or issues of reputational risk.[6]
- If the breach does not need to be reported to the Leadership Team to action the IT Consultant investigates fully how the breach occurred, what information was breached, how the breach can be ameliorated and how to prevent future breaches. The Adverse Event Report is updated.

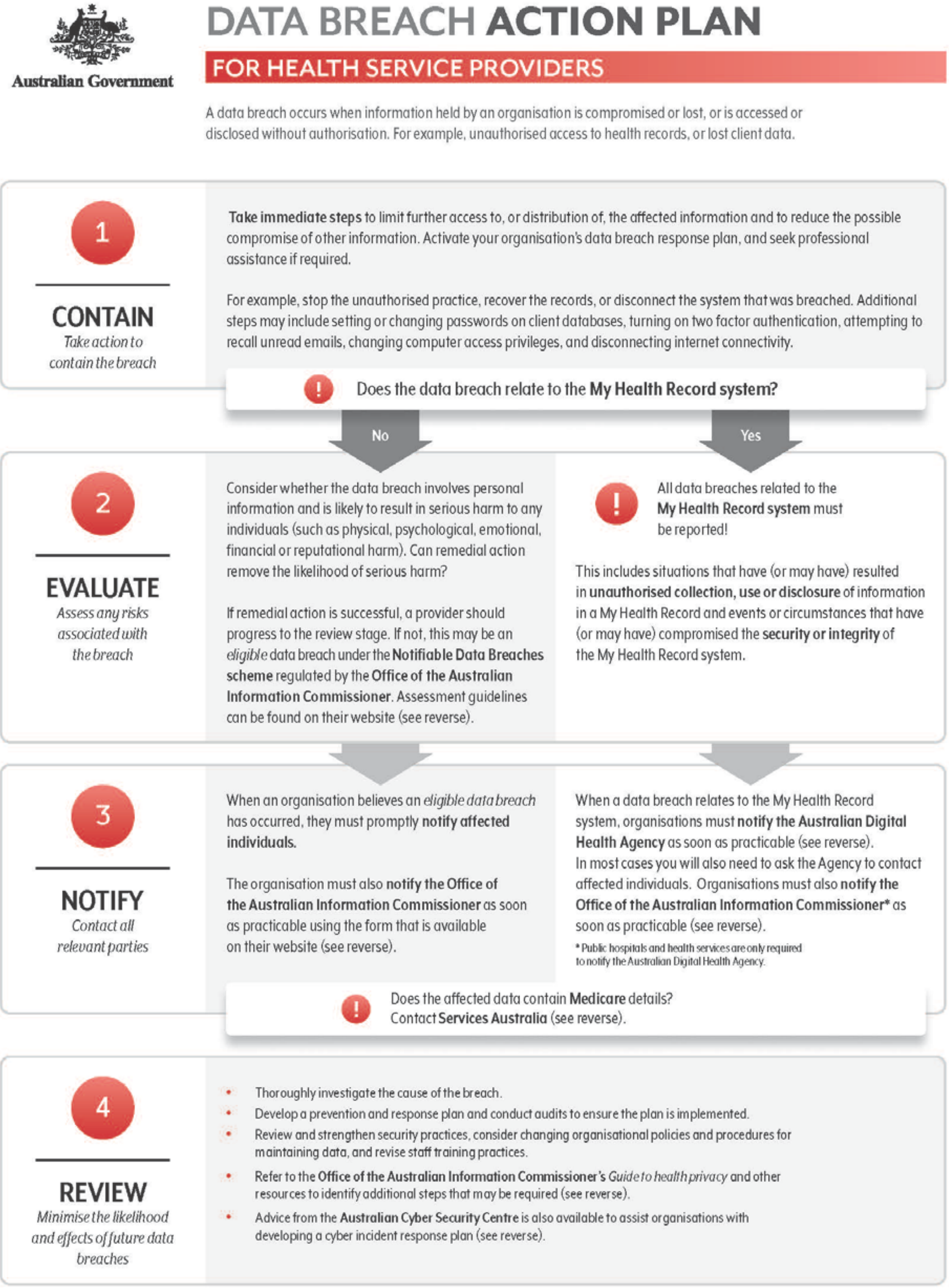
[6] These items are included on the Data Breach Report

- The IT Consultant provides a report to the CEO for review, which is then reported to the Leadership Team as required.
- The Leadership Team determines if the breach must be reported to the Commissioner under the Notifiable Data Breaches (NDB) scheme. This is determined on the factors noted above in Notifiable Data Breaches[7] and in consideration of Figure: 8.11.2: OAIC Data Breach Action Plan for Health Service Providers. The CEO lodges the report and updates the Adverse Event Report.
- The Leadership Team determines if the breach must be reported to any other authorities and lodges the report/s. (See Notifiable Data Breaches above for a list of possible agencies to be notified[8].) The Leadership Team updates the Adverse Event Report.
- If the Leadership Team determines that it is likely that any person's data is at risk of being viewed or utilised by others, a member of the Team ensures that the person/s are advised of the type of data breached, action taken, potential consequences and what we have done to ensure it does not occur again. Advice may be written, verbal or face to face or a combination, depending on the breach and consequences.
- In the event of unlawful access to data on the IT system the system is immediately isolated and the IT consultant is requested to identify the extent of the breach, recover lost information if possible, secure the system, determine how the breach occurred and how to prevent it in the future.
- The Data Breach Report is updated by the IT Consultant and processed and closed out by the Improvement Committee as per KCSP014 8.9.8 Processing Continuous Improvement Forms and Other Improvement Information. The Improvement Committee reviews the data breach and the appropriateness of the response and considers if any improvements can be made to the data breach process.
- The CEO reports all data breaches to the next Board of Management Meeting. (See Table KCSP007 8.3.1: Management Meetings/Board of Management Meetings.)

[7] These items are included on the Data Breach Report

[8] These agencies are included on the Data Breach Report

Figure 8.11.2: OAIC Data Breach Action Plan for Health Service Providers



Australian Government

DATA BREACH ACTION PLAN

FOR HEALTH SERVICE PROVIDERS

A data breach occurs when information held by an organisation is compromised or lost, or is accessed or disclosed without authorisation. For example, unauthorised access to health records, or lost client data.

1

CONTAIN
Take action to contain the breach

Take immediate steps to limit further access to, or distribution of, the affected information and to reduce the possible compromise of other information. Activate your organisation's data breach response plan, and seek professional assistance if required.

For example, stop the unauthorised practice, recover the records, or disconnect the system that was breached. Additional steps may include setting or changing passwords on client databases, turning on two factor authentication, attempting to recall unread emails, changing computer access privileges, and disconnecting internet connectivity.

! Does the data breach relate to the **My Health Record system?**

No

Yes

2

EVALUATE
Assess any risks associated with the breach

Consider whether the data breach involves personal information and is likely to result in serious harm to any individuals (such as physical, psychological, emotional, financial or reputational harm). Can remedial action remove the likelihood of serious harm?

If remedial action is successful, a provider should progress to the review stage. If not, this may be an *eligible* data breach under the **Notifiable Data Breaches scheme** regulated by the **Office of the Australian Information Commissioner**. Assessment guidelines can be found on their website (see reverse).

! All data breaches related to the **My Health Record system** must be reported!

This includes situations that have (or may have) resulted in **unauthorised collection, use or disclosure** of information in a My Health Record and events or circumstances that have (or may have) compromised the **security or integrity** of the My Health Record system.

3

NOTIFY
Contact all relevant parties

When an organisation believes an *eligible data breach* has occurred, they must promptly **notify affected individuals.**

The organisation must also **notify the Office of the Australian Information Commissioner** as soon as practicable using the form that is available on their website (see reverse).

When a data breach relates to the My Health Record system, organisations must **notify the Australian Digital Health Agency** as soon as practicable (see reverse). In most cases you will also need to ask the Agency to contact affected individuals. Organisations must also **notify the Office of the Australian Information Commissioner*** as soon as practicable (see reverse).

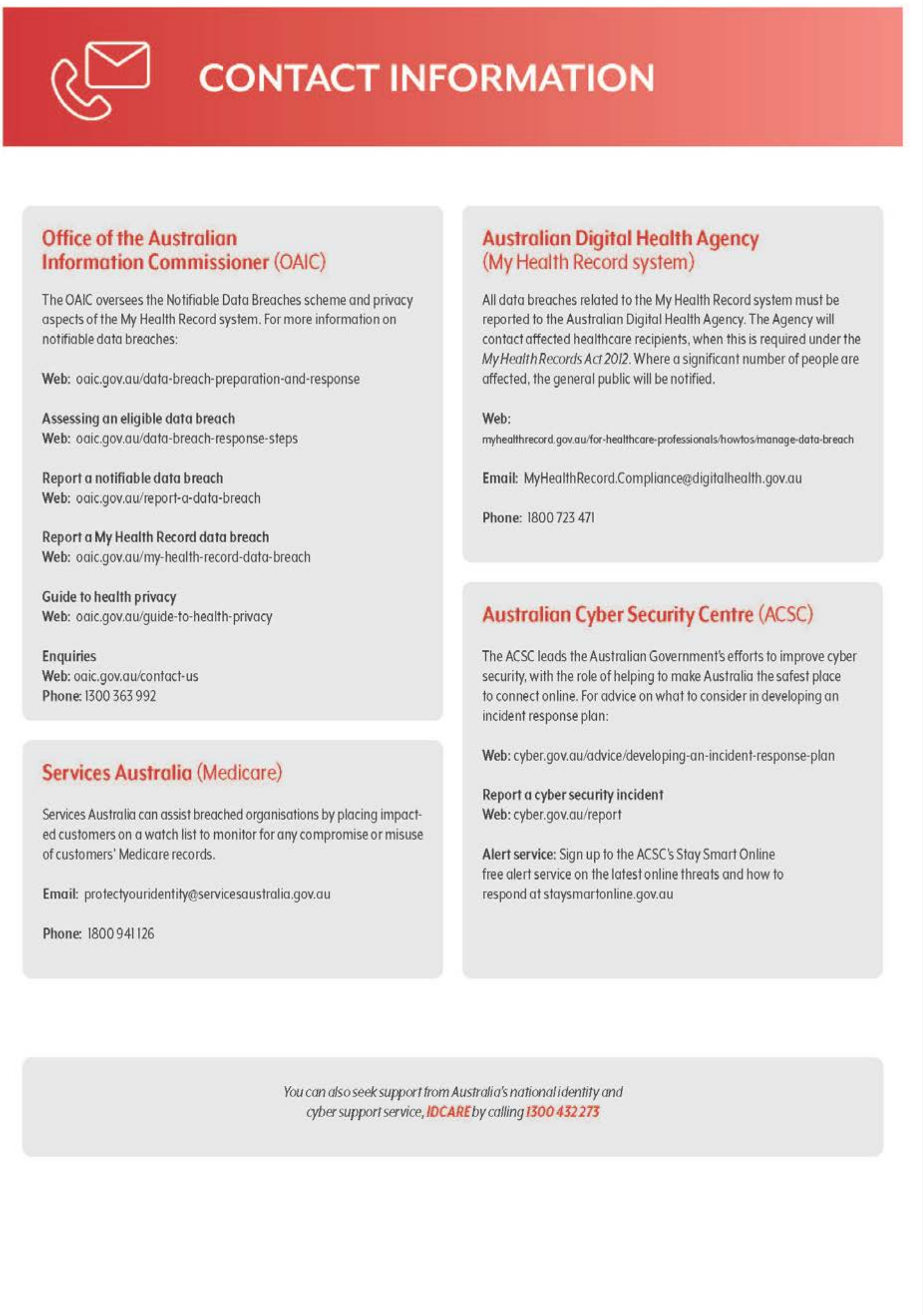
* Public hospitals and health services are only required to notify the Australian Digital Health Agency.

! Does the affected data contain **Medicare** details? Contact **Services Australia** (see reverse).

4

REVIEW
Minimise the likelihood and effects of future data breaches

- Thoroughly investigate the cause of the breach.
- Develop a prevention and response plan and conduct audits to ensure the plan is implemented.
- Review and strengthen security practices, consider changing organisational policies and procedures for maintaining data, and revise staff training practices.
- Refer to the **Office of the Australian Information Commissioner's** *Guide to health privacy* and other resources to identify additional steps that may be required (see reverse).
- Advice from the **Australian Cyber Security Centre** is also available to assist organisations with developing a cyber incident response plan (see reverse).



CONTACT INFORMATION

Office of the Australian Information Commissioner (OAIC)

The OAIC oversees the Notifiable Data Breaches scheme and privacy aspects of the My Health Record system. For more information on notifiable data breaches:

Web: oaic.gov.au/data-breach-preparation-and-response

Assessing an eligible data breach
Web: oaic.gov.au/data-breach-response-steps

Report a notifiable data breach
Web: oaic.gov.au/report-a-data-breach

Report a My Health Record data breach
Web: oaic.gov.au/my-health-record-data-breach

Guide to health privacy
Web: oaic.gov.au/guide-to-health-privacy

Enquiries
Web: oaic.gov.au/contact-us
Phone: 1300 363 992

Services Australia (Medicare)

Services Australia can assist breached organisations by placing impacted customers on a watch list to monitor for any compromise or misuse of customers' Medicare records.

Email: protectyouridentity@servicesaustralia.gov.au

Phone: 1800 941 126

Australian Digital Health Agency (My Health Record system)

All data breaches related to the My Health Record system must be reported to the Australian Digital Health Agency. The Agency will contact affected healthcare recipients, when this is required under the *My Health Records Act 2012*. Where a significant number of people are affected, the general public will be notified.

Web:
myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach

Email: MyHealthRecord.Compliance@digitalhealth.gov.au

Phone: 1800 723 471

Australian Cyber Security Centre (ACSC)

The ACSC leads the Australian Government's efforts to improve cyber security, with the role of helping to make Australia the safest place to connect online. For advice on what to consider in developing an incident response plan:

Web: cyber.gov.au/advice/developing-an-incident-response-plan

Report a cyber security incident
Web: cyber.gov.au/report

Alert service: Sign up to the ACSC's Stay Smart Online free alert service on the latest online threats and how to respond at staysmartonline.gov.au

*You can also seek support from Australia's national identity and cyber support service, **IDCARE** by calling **1300 432 273***

Testing of the Data Breach Response Plan

Ongoing testing of different scenarios of data breaches is carried out regularly as part of our risk management process. This may involve staff and our IT Consultant.

(See KCSP015 8.10.3 Risk Management Plans.)

(See KCSP021 7.4.3 Staff Education/Mandatory Training.)

RECORD OF REVISIONS

Unless the Policy specifically states otherwise, the Policy does not form part of your employment agreement with KCS. KCS may unilaterally vary, remove or replace this Policy at any time. To the extent that this Policy imposes any obligations on KCS and/or purports to provide any right or benefit to you, those obligations are not contractual and do not give rise to any contractual rights. The Employee is required to be familiar with the content of the Policy and comply with the terms at all times.

File Reference	KCSP016 – Information Management				
Date Created	15/11/2021	Created By	Marisa Turcinskis	Responsible	CEO

Version Number	Modified or Reviewed by	Modifications Made/Notes	Date	STATUS (Internal, External, Archived)
V1	MT	GGJ Version - Formatted to reflect KCS branding. IT MYway consulted.	15/11/2021	DRAFT
V2	MT	GGJ Update 17/11/21	19/11/21	DRAFT
V3	MT	GGJ Split	13/5/22	DRAFT
V4	MT	Originated from GGJ ACP811 made into whole of KCS doc	9/6/22	DRAFT
V5	Board	Ratified at Board meeting	29/8/22	Live