**CDR Policy Requirements   
Cross-Reference Matrix**

|  |
| --- |
| Disclaimer: The information in this document is provided “as is” with no guarantee of completeness |

Provided by Regional Australia Bank   
to the CDR Community in August 2020

**Last updated: 15 August 2020**

**Known Requirements for CDR Policy Development**

**Document Purpose**

This document is intended to be used as a starter mechanism for CDR participants to help understand, track, confirm and communicate compliance with known obligations in respect of CDR Policy development. It covers obligations defined in the CDR Rules, the CDR Rules Explanatory Statement and the Act. It was used by Regional Australia Bank to develop a CDR policy as an early participant of the Australian CDR in July 2020.

The outcome of this work is available online in interactive and static formats at:

<https://www.regionalaustraliabank.com.au/our-cdr-policy>

**How to use this document**

Modify the last 3 columns of each of the horizontal-format tables provided below. Update with comments relevant to your CDR use case. Set the colour and contents of the last 2 columns to allow tracking of those items that require further work or are not complete.

Comments within the tables below may not apply to your individual business circumstances or use case. They are left in place in the hope that they may assist in some way with understanding.

**Definitions**

**CDR Policy** means a policy that a CDR participant has and maintains in compliance with subsection 56ED(3) of the Act.

**Act** means the Competition and Consumer Act 2010.   
*Note the main part we need to be concerned with is Division 5 – Privacy Safeguards, Subdivision A – Preliminary which includes 56EA through section 56EZ (pages 377-406)*

**Rules** means the Competition and Consumer (Consumer Data Right) Rules (February 2020) *Note the main source of information relating to the CDR Policy appears in Subdivision 7.2.1 – Rules relating to consideration of CDR data privacy*

**Resources**

**CDR Rules (February 2020)**  
<https://www.accc.gov.au/system/files/CDR%20Rules%20-%20Final%20-%206%20February%202020.pdf>

**Rules Explanatory Statement (February 2020)**<https://www.accc.gov.au/system/files/CDR%20Rules%20Explanatory%20Statement%20-%206%20February%202020.pdf>

**OAIC Guide to developing a CDR policy (June 2020)**<https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/guide-to-developing-a-cdr-policy/>

**The Following Tables**

The following pages show **three** tables – one for each of the two major legislative CDR documents - the CDR Rules and the Act and a table for additional content provided in the CDR Rules Explanatory Statement

The tables include every known identified clause that has a reference to, or is associated with, the definition of a *CDR Policy*. Where references are made between documents, this is shown in the tables.

Where Rules or requirements only apply to a Data Holder or a Data Recipient, they are tagged as follows:

|  |  |
| --- | --- |
| **A picture containing object, clock, drawing  Description automatically generated** | Rules that only apply to Data Holders |
| **A picture containing drawing  Description automatically generated** | Rules that only apply to Data Recipients |

The assumption is, if a CDR Policy addresses all these clauses, it will be deemed compliant by the ACCC as part of the accreditation process.

**CDR Policy Requirements Cross-Reference**

**CDR Rules (February 2020)**

| **DR DH** | **Ref** | **Content** | **Our Comment** | **Do we fully understand this?** | **Does our CDR Policy comply?** |
| --- | --- | --- | --- | --- | --- |
|  | *Policy about the management of CDR data* | | | |  |
|  | **Rules 7.2 (1)** | For paragraph 56ED(3)(b) of the Act, the Information Commissioner may approve a form for a CDR policy. | There is currently no defined or approved form for a CDR Policy  There is some really helpful content in here, especially in Step 2 – Develop content, structure and presentation (don’t consider this policy to need to be like any existing policy)  <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/guide-to-developing-a-cdr-policy/>  The policy will be reviewed by the ACCC as part of the DR accreditation process | Yes | N/A |
|  | **Rules 7.2 (2)** | For paragraph 56ED(3)(b) of the Act, a CDR entity's CDR policy must be in the form of a document that is distinct from any of the CDR entity's privacy policies. | We need to create a separate CDR policy; we can’t adapt an existing policy. The reference in the act states “…is in a form approved in accordance with the consumer data rules…”  We will have a single policy for CDR covering both DH and DR. | Yes | Yes |
|  | *Additional information for CDR policy* | | | |  |
|  | **Rules 7.2 (3)** | In addition to the information referred to in subsection 56ED(4) of the Act, a data holder's CDR policy must indicate: | | |  |
| **A picture containing object, clock, drawing  Description automatically generated** | (a) | whether it accepts requests for:   1. voluntary product data; or 2. voluntary consumer data; and | Voluntary data is data outside the scope of CDR and is aimed to allow DHs to offer additional information to DRs. | Yes | Not Fully |
| **A picture containing object, clock, drawing  Description automatically generated** | (b) | if so:   1. whether it charges fees for disclosure of such data; and 2. if it does-how information about those fees can be obtained. | We need to decide if fees may be charged for disclosure of voluntary data. | Yes | No |
|  | **Rules 7.2 (4)** | In addition to the information referred to in subsection 56ED(5) of the Act, an accredited data recipient's CDR policy must: | | |  |
| **A picture containing drawing  Description automatically generated** | (a) | include a statement indicating the consequences to the CDR consumer if they withdraw a consent to collect and use CDR data; and | Depending on when consent is withdrawn, this might mean it is not possible to provide some services to the consumer. No fees will be charged for this. |  |  |
| **A picture containing drawing  Description automatically generated** | (b) | include a list of the outsourced service providers (whether based in Australia or based overseas, and whether or not any is an accredited person); and | This ensures DRs are being transparent about who is involved in delivering the service using CDR data so consumers can make an informed choice. It also provides an opportunity to support business partners. |  |  |
| **A picture containing drawing  Description automatically generated** | (c) | for each such service provider-include:   1. the nature of the services it provides; and 2. the CDR data or classes of CDR data that may be disclosed to it; and | Consider putting high level content in the policy and then linking to a separate page with more OSP details so the policy remains succinct.  <https://www.regionalaustraliabank.com.au/personal/support/outsourced-service-providers> |  |  |
| **A picture containing drawing  Description automatically generated** | (d) | if the accredited data recipient is likely to disclose CDR data of a kind referred to in subsection 56ED(5) of the Act to such a service provider that:   1. is based overseas; and 2. is not an accredited person;   include the countries in which such persons are likely to be based if it is practicable to specify those countries in the policy; and | If this doesn’t apply, then it can be dealt with a single blanket statement – for example ‘we do not use overseas service providers’. |  |  |
| **A picture containing drawing  Description automatically generated** | (e) | if applicable-include the following information about de-identification of CDR data that is not redundant data:   1. how the accredited person uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to CDR consumers; 2. the further information specified in subrule (5); and | Check subrule (5)  Redundant data is defined in the Rules as being defined in the Act 56EO. That definition is a little ambiguous but basically states that once the original purpose has been achieved and there is no other reason to retain it, it becomes redundant.  Remember that even if raw CDR data has been transformed into something else, the fact that it was derived from CDR data means that it is still CDR data, and it might not be redundant data. In some use cases it might be necessary to retain this information, perhaps for statutory or other reasons. |  |  |
| **A picture containing drawing  Description automatically generated** | (f) | include the following information about deletion of redundant CDR data:   1. when it deletes redundant data; 2. how a CDR consumer may elect for this to happen; 3. how it deletes redundant data; and | This will potentially vary by use case so perhaps challenging to provide in a single policy that applies to all such cases.  With one-time consent for lending, we propose to delete all redundant data, consumers *could* elect for this to happen earlier although this would likely then impact our ability to deliver the service.  As our use case doesn’t involve holding redundant data, the only data that could be deleted would that which is still serving the purpose for which consent was originally provided.  Information on how redundant data is deleted is aimed to provide greater consumer transparency. This needs to be balanced with the need to maintain appropriate data security.  Section **56EO** of the Act, states:  *If:*  *(a) the CDR entity no longer needs any of that CDR data for either of the following purposes (the* ***redundant data****):*  *(i) a purpose permitted under the consumer data rules;*  *(ii) a purpose for which the person is able to use or disclose it in accordance with this Division; and*  *(b) the CDR entity is not required to retain the redundant data by or under an Australian law or a court/tribunal order; and*  *(c) the redundant data does not relate to any current or anticipated:*  *(i) legal proceedings; or*  *(ii) dispute resolution proceedings;*  *to which the CDR entity is a party;*  *the CDR entity must take the steps specified in the consumer data rules to destroy the redundant data or to ensure that the redundant data is de-identified.*  So, we need to consider how the situation might change if someone is no longer a customer? Does that change perspective and obligation here?  Consider whether there is any statutory obligation to retain redundant data – perhaps to justify decisions if challenged at a later date. |  |  |
| **A picture containing drawing  Description automatically generated** | (g) | if applicable-include the following information about de-identification of redundant CDR data:   1. if the de-identified data is used by the accredited data recipient- examples of how the accredited data recipient ordinarily uses de-identified data; and 2. the further information specified in subrule (5); and | It may be simpler to delete all data once it becomes redundant and just state this. |  |  |
| **A picture containing drawing  Description automatically generated** | (h) | include the following information about the CDR consumer's election to delete their CDR data:   1. information about how the election operates and its effect; 2. information about how CDR consumers can exercise the election. | For example, state that when a consumer withdraws consent, all data will be permanently deleted, and that consent can be managed through our consumer dashboard at https://... or by  Election to delete could be done using the consumer dashboard, or by contacting us using our online form at https://... or by calling our contact centre on 132… |  |  |
| **A picture containing drawing  Description automatically generated** | Note 1 | The specified service providers are the accredited data recipient's "outsourced service providers". | Rule 1.10 states: *For these rules, an outsourced service provider is a person to whom an accredited person discloses CDR data under a CDR outsourcing arrangement.*  Make sure we have a written agreement with any third party to whom we disclose CDR data, that is compliant with the various clauses specified in Rule 1.10 |  | No policy content required |
| **A picture containing drawing  Description automatically generated** | Note 2 | For paragraph (d), if the service provider is an accredited person who is based overseas, paragraph 56ED(5)(f) of the Act requires similar information to be contained in the accredited data recipient's CDR policy. | This won’t apply if OSPs aren’t based overseas. It can be dealt with via a blanket statement advising ‘we don’t outsource to overseas service providers’. |  |  |
| **A picture containing drawing  Description automatically generated** | Note 3 | This subrule is a civil penalty provision (see rule 9.8). | Rule 9.8 lists all the clauses that have civil penalty provisions (within the meaning of the Regulatory Powers Act). There are lots… |  | No policy content required |
|  | **Rules 7.2 (5)** | For subparagraphs (4)(e)(ii) and (g)(ii), the further information is: | | |  |
| **A picture containing drawing  Description automatically generated** | (a) | how the accredited person de-identifies CDR data, including a description of techniques that it uses to de-identify data; and | This needs to have some reasonable depth to it, but avoid going into detailed technical that won’t be beneficial to consumers and may confuse them. |  |  |
| **A picture containing drawing  Description automatically generated** | (b) | if the accredited person ordinarily discloses (by sale or otherwise) de-identified data to one or more other persons:   1. that fact; and 2. to what classes of person it ordinarily discloses such data; and 3. why it so discloses such data. | We can’t find a definition of classes of person in the Rules. The Act references them in 56BA(2) but there is no definition.  Subsequent guidance from the OAIC is that *“Entities or persons do not need to be listed individually in the CDR policy, but should be described with enough specificity so that the consumer can understand the nature of those parties who will hold or have access to de-identified data. Examples of ‘classes of persons’ could be insurance companies, market research providers, data analytics services”* |  |  |
|  | **Rules 7.2 (6)** | In addition to the information referred to in paragraphs 56ED(4)(b) and (5)(d) of the Act, a CDR participant's CDR policy must include the following information in relation to the participant's internal dispute resolution processes: | | |  |
|  | (a) | where a CDR consumer complaint can be made; | At any of our locations, online via website, online via application form, calling contact centre on 1300… |  |  |
|  | (b) | how a CDR consumer complaint can be made; | Consider emulating existing AFCA dispute resolution scheme and align processes.  Likely requirement to update existing internal complaints procedure and provide training to staff.  Likely to require additional complaints categories to be defined in readiness for reporting once live. |  |  |
|  | (c) | when a CDR consumer complaint can be made; | Consider emulating existing AFCA dispute resolution scheme and align processes.  Likely to be at one of our locations or via phone during business hours, or online via the web and application form 24/7  Consider having a dedicated Feedback and Complaints section on the public website. |  |  |
|  | (d) | when acknowledgement of a CDR consumer complaint can be expected; | Consider emulating existing AFCA dispute resolution scheme and align processes unless the rules determine timeframes,  CDR policy should refer to our Internal Dispute Resolution Process which specifies that complaints will be resolved as quickly as possible however specifies required notices to be issued at 5 days, 21 days and 45 days.  CDR Rules do not express a required timeframe, but reporting requires a report on the number of complaints resolved within 5 days. |  |  |
|  | (e) | what information is required to be provided by the complainant | Consider using a statement such as “For the purpose of resolving your complaint we may ask for your personal information, including your name, contact information and the details of your complaint” |  |  |
|  | (f) | the participant's process for handling CDR consumer complaints; | Consider emulating existing AFCA dispute resolution scheme and align processes.  Update complaints handling documentation on public website to reference CDR complaints. |  |  |
|  | (g) | time periods associated with various stages in the CDR consumer complaint process; | Consider emulating existing AFCA dispute resolution scheme and align processes.  Update complaints handling documentation on public website to reference CDR complaints. |  |  |
|  | (h) | options for redress; | Consider emulating existing AFCA dispute resolution scheme and align processes.  Update complaints handling documentation on public website to reference CDR complaints. |  |  |
|  | (i) | options for review, both internally (if available) and externally | Consider emulating existing AFCA dispute resolution scheme and align processes.  Update complaints handling documentation on public website to reference CDR complaints. |  |  |
|  | Note | This subrule is a civil penalty provision (see rule 9.8). | Rule 9.8 lists all the clauses that have civil penalty provisions (within the meaning of the Regulatory Powers Act) |  | N/A |
| **A picture containing drawing  Description automatically generated** | **Rules 7.2 (7)** | If an accredited data recipient proposes to store CDR data other than in Australia or an external territory, its CDR policy must specify any country in which they propose to store CDR data. | Provide a statement such as:  *We do not use any overseas outsourced providers for CDR data activities. Your data will not leave Australia.* |  |  |
| **A picture containing drawing  Description automatically generated** | Note | This subrule is a civil penalty provision (see rule 9.8). | Rule 9.8 lists all the clauses that have civil penalty provisions (within the meaning of the Regulatory Powers Act) |  | No policy content required |
|  | *Availability of policy* | | | |  |
|  | **Rules 7.2 (8)** | For paragraph 56ED(7)(b) of the Act, a CDR participant must make its CDR policy readily available through each online service by means of which the CDR participant ordinarily deals with CDR consumers. | Some subjectivity here however the guidance suggests that if the interaction ordinarily happens thorough a particular online platform then the policy should be provided through that channel. |  | No policy content required |
|  | Note | This subrule is a civil penalty provision (see rule 9.8). | Rule 9.8 lists all the clauses that have civil penalty provisions (within the meaning of the Regulatory Powers Act) |  | No policy content required |
|  | **Rules 7.2 (9)** | For subsection 56ED(8) of the Act, if a copy of a the CDR participant's policy is requested by a CDR consumer, the participant must give the CDR consumer a copy: | | |  |
|  | (a) | electronically; or | Provide via the website in HTML and also static PDF as required. |  |  |
|  | (b) | in hard copy;  as directed by the consumer. | We can print this out at office locations if a customer needs it, or we could provide via mail. |  |  |
|  | Note | This subrule is a civil penalty provision (see rule 9.8). | Rule 9.8 lists all the clauses that have civil penalty provisions (within the meaning of the Regulatory Powers Act). |  | No policy content required |

**CDR Policy Requirements Cross-Reference**

**Aligned with the Competition and Consumer Act (including amendments up to: Act No. 94, 2019)**

| **DR DH** | **Ref** | **Content** | **Comment** | **Do we fully understand this?** | **Does our CDR Policy comply?** |
| --- | --- | --- | --- | --- | --- |
|  | *Policy about the management of CDR data* | | | | |
|  | **Act 56ED(3)** | The CDR entity must have and maintain a clearly expressed and up-to-date policy that: | | | |
|  | (a) | is about the CDR entity’s management of CDR data; and |  | Yes | N/A |
|  | (b) | is in a form approved in accordance with the consumer data rules; and | Referenced in Rules 7.2 (1)  There is currently no defined or approved form for a CDR Policy  There is some really helpful content in here, especially in Step 2 – Develop content, structure and presentation (don’t consider this policy to need to be like any existing policy)  <https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/guide-to-developing-a-cdr-policy/>  The policy will be reviewed by the ACCC as part of the DR accreditation process | Yes | Yes |
|  | **Act 56ED(4)** | If the CDR entity is a **data holder** of any CDR data, the CDR entity’s policy must contain the following information: | | | |
| **A picture containing object, clock, drawing  Description automatically generated** | (a) | how a CDR consumer for the CDR data may access the CDR data and seek the correction of the CDR data; | As a DR this doesn’t apply to us yet and our use case but these will be needed down the track so we will include. | Yes | Not Yet |
| **A picture containing object, clock, drawing  Description automatically generated** | (b) | how a CDR consumer for the CDR data may complain about a failure of the CDR entity to comply with this Part or the consumer data rules, and how the CDR entity will deal with such a complaint. | As a DR this doesn’t apply to us yet and our use case but these will be needed down the track so we will include.  See Rule 7.2(6) on dispute resolution | No | Not Yet |
|  | **Act 56ED(5)** | If the CDR entity is an accredited data recipient of any CDR data, the CDR entity’s policy must contain the following information:  *Referenced in Rules 7.2 (4), 7.2 (4)(d)* | | | |
| **A picture containing drawing  Description automatically generated** | (a) | the classes of CDR data held by (or on behalf of) the CDR entity as an accredited data recipient, and how such CDR data is held; | Need to understand what is meant by classes and therefore how we hold this data  The Consumer Data Right (Authorised Deposit‑Taking Institutions) Designation 2019 (the Designation) sets out three classes of information for the banking sector: customer information, product use information, and Information on the product.  This relates to clusters described in the consent flow of the UI and will require an associated statement such as “We may collect up to three types of CDR Data – account product information, account balances and account transactions.” |  |  |
| **A picture containing drawing  Description automatically generated** | (b) | the purposes for which the CDR entity may collect, hold, use or disclose such CDR data with the consent of a CDR consumer for the CDR data; | The purpose is defined by the use case and associated software application so again, hard to be generic here at policy level but something like this might be appropriate in our use case:  “We are requesting access to your data in order to help us better understand your personal financial situation. Having access to this data helps us analyse your spending and saving habits to provide insights into your financial health and to assist with your loan application.”  Another example might be “…and detect unusual transactions that might be fraudulent…” |  |  |
| **A picture containing drawing  Description automatically generated** | (c) | how a CDR consumer for such CDR data may access the CDR data and seek the correction of the CDR data; | In our use case, the raw CDR data does not survive the transformation, however this would appear more relevant to a data holder than a recipient given that only the DH could correct the source data. |  |  |
| **A picture containing drawing  Description automatically generated** | (d) | how a CDR consumer for such CDR data may complain about a failure of the CDR entity to comply with this Part or the consumer data rules, and how the CDR entity will deal with such a complaint; | Referenced extensively in Rules 7.2 (6) |  |  |
| **A picture containing drawing  Description automatically generated** | (e) | whether the CDR entity is likely to disclose such CDR data to accredited persons who are based overseas; | Not applicable to our use case so we can state that data will not leave Australia |  |  |
| **A picture containing drawing  Description automatically generated** | (f) | if the CDR entity is likely to disclose such CDR data to accredited persons who are based overseas—the countries in which such persons are likely to be based if it is practicable to specify those countries in the policy; | Not applicable, see (e) above |  |  |
| **A picture containing drawing  Description automatically generated** | (g) | the circumstances in which the CDR entity may disclose such CDR data to a person who is not an accredited person; | We need to declare that we will disclose de-identified data to an outsourced service provider as described in response to Rule 7.2(4)(b) |  |  |
| **A picture containing drawing  Description automatically generated** | (h) | the events about which the CDR entity will notify the CDR consumers of such CDR data; | This is a confusing clause; it is not clear if this relates to (g) above or more broadly. Not clear what ‘such CDR data’ refers to. | Not Really | Not Sure |
| **A picture containing drawing  Description automatically generated** | (i) | the circumstances in which the CDR entity must delete or de-identify such CDR data in accordance with a request given by a CDR consumer for the CDR data under the consumer data rules. | Covered in Rules 7.2(5)(a) |  |  |
|  | **Act 56ED(7)** | The CDR entity must make the CDR entity’s policy available: | | | |
|  | (a) | free of charge; and | This is consistent with other bank documents such as the privacy policy. This is not an issue. This is stated in the CDR policy. |  |  |
|  | (b) | in accordance with the consumer data rules. | See comments in Rules table above |  |  |
|  | Note | Note: One way the consumer data rules could require the policy to be made available is to require the policy to be made available in accordance with a data standard. | There isn’t a current known data standard to be applied to the policy, so this does not appear to be relevant at present. | No Fully |  |
|  | **Act 56ED(8)** | If a copy of the CDR entity’s policy is requested by a CDR consumer for the CDR data, the CDR entity must give the CDR consumer a copy in accordance with the consumer data rules. | This is consistent with other bank documents such as the privacy policy. This is not an issue.  Referenced in Rules 7.2 (9) |  |  |

**CDR Policy Requirements Cross-Reference**

**CDR Rules Explanatory Statement (February 2020)**

| **DR DH** | **Ref** | **Content** | **Comment** | **Do we fully understand this?** | **Does our CDR Policy comply?** |
| --- | --- | --- | --- | --- | --- |
|  | *Division 7.2 – Rules relating to privacy safeguards,* Subdivision 7.2.1 – Rules relating to consideration of CDR data privacy Privacy Safeguard 1 – open and transparent management of CDR data Rule 7.2 | | | |  |
|  | **ES 212** | Data holders and accredited data recipients are required to have a policy about the management of CDR data that they make readily available online (CDR policy). Section 56ED of the Act sets out the matters that the policy must contain. The rules set out additional information that the policy must contain and how it should be made available to consumers. | See comments for Rule 7.2(1) and (2)  Clauses in these 3 cross-reference tables will ensure compliance with Rules and the Act. | Yes | No policy content required |
|  | **ES 213** | A CDR policy is taken to be in the approved form if it follows the approach to content and structure set out in OAIC Guidelines, or any other guidance on Privacy Safeguard 1 referred to in those Guidelines. A CDR policy must be a separate document to the entity’s general privacy or other policies. Where a person is both an accredited data recipient and a data holder, the person may have two separate CDR policies or a single CDR policy, provided that the information contained covers the person acting in both capacities. | See comments for Rule 7.2(1) and (2) | Yes | Not Fully |
| **A picture containing object, clock, drawing  Description automatically generated** | **ES 214** | A data holder’s CDR policy must indicate whether it accepts requests for voluntary product or consumer data and, if so, the types of such data that can be requested, whether it charges a fee for the disclosure of such data and, if it does, how information about those fees can be obtained. This is to assist CDR consumers in knowing what data can be accessed. It also will help inform accredited data recipients as to whether they can see a CDR consumer’s consent for the disclosure of such voluntary data and any fees that may be applicable. | See comments for Rule 7.2(3) | Yes | Not Fully |
| **A picture containing drawing  Description automatically generated** | **ES 215** | The CDR policy must also inform consumers of what the consequences will be, if any, if they withdraw their consent during the consent period. This, for example, could include information about any early cancellation fees. | See comment for Rule 7.2(4)(a) | Yes | Not Yet |
| **A picture containing drawing  Description automatically generated** | **ES 216** | The policy must provide a list of outsourced service providers used by the accredited data recipient, the nature of the services they provide, and the types of data that may be disclosed to those outsourced service providers. If any of the outsourced service providers are based overseas and are not accredited themselves, the accredited data recipient must include the countries in which those outsourced service providers are based. If an accredited data recipient proposes to disclose CDR data overseas, its CDR policy must specify in which countries it proposes to disclose CDR data. | See comment for Rule 7.2(4)(b) and (c) | Partly | Not Yet |
| **A picture containing drawing  Description automatically generated** | **ES 217** | The policy is also intended, in addition to the consent process, to give consumers transparency around the de-identification and destruction of CDR data processes. | See comment for Rule 7.2(4)(e),(f) and (g) |  |  |
| **A picture containing drawing  Description automatically generated** | **ES 218** | For de-identification that occurs as a use of CDR data that is consented to in order to disclose (by sale or otherwise) de-identified CDR data, accredited data recipients must include information about: | | | |
|  | (a) | how the accredited person uses CDR data that has been de-identified in accordance with the CDR data de-identification process to provide goods or services to CDR consumers; and | See comment for Rule 7.2(4)(e) |  |  |
|  | (b) | The further information specified in paragraph 221 below. | This is about de-identification |  |  |
| **A picture containing drawing  Description automatically generated** | **ES 219** | For the treatment of redundant data, the policy must include information on: | | | |
|  | (a) | the following information about deletion of redundant data:   1. when the accredited data recipient deletes redundant data 2. how a CDR consumer may elect for this to happen 3. how the redundant data is deleted; and | See comment for Rule 7.2(4)(e) |  |  |
|  | (b) | if applicable – the following information about de-identification of redundant CDR data:   1. if the de-identified is used by the accredited data recipient, examples of how the accredited data recipient ordinarily uses de-identified data; and 2. the further information specified in paragraph 221 below. | This is again going to be very specific to each use case. |  |  |
| **A picture containing drawing  Description automatically generated** | **ES 220** | The policy must also include information about the CDR consumer’s election to delete, being: | | | |
|  | (a) | information about how the election operates and its effect; and |  |  |  |
|  | (b) | information about how CDR consumers can exercise the election. | See comment for Rule 7.2(4)(f) and (h) |  |  |
| **A picture containing drawing  Description automatically generated** | **ES 221** | The further information about de-identification is: | | | |
|  | (a) | How the accredited person de-identifies CDR data, including a description of the techniques it uses; and | See comment for Rule 7.2(4)(e) and (g) |  |  |
|  | (b) | If the accredited person ordinarily discloses (by sale or otherwise) deidentified data to one or more persons:   1. that fact; and 2. to what classes of persons it ordinarily discloses such data; and 3. why it so discloses such data. | See comment for Rule 7.2(5)(b) |  |  |
|  | **ES 222** | Accredited data recipients and data holders must also include information in their CDR policies about their internal dispute resolution processes, including how a complaint can be made and the participant’s process for handling CDR consumer complaints. | See comment for Rule 7.2(6) |  |  |
| **A picture containing drawing  Description automatically generated** | **ES 223** | If an accredited data recipient proposes to store CDR data other than in Australia or an external territory, its CDR policy must specify any country in which it proposes to store CDR data. | See comment for Rule 7.2(7) |  |  |