CDR Rules Expansion Amendments | Illustrative Wireframes

Overview

The Consumer Data Right (CDR) gives consumers greater control over their data, empowering them to share their data with trusted recipients for the purposes they have authorised.

The Australian Competition and Consumer Commission (ACCC) developed the CDR Rules to facilitate CDR as an economy-wide right. The ACCC is now consulting on proposed new rules to build on the foundational CDR Rules.

To facilitate engagement and comprehension of the proposed new rules, the Data Standard Body's (DSB) Consumer Experience (CX) Working Group, in collaboration with the ACCC, has developed wireframes based on key rules enhancements.

The wireframes contained in this document have been developed to illustrate how the proposed new rules could work in practice.

This document should be read in conjunction with the CDR Rules Exposure Draft and the CDR Rules Expansion Amendments consultation paper. The community should expect these wireframes to evolve based on further iterations and in line with how the proposed rules consultation progresses.

***NB** These wireframes were developed to illustrate how the proposed new rules could work in practice, but are not to be taken as compliant examples of these rules.*

Stakeholders should not rely on these wireframes to demonstrate compliance with the proposed rules, once made.

If the example wireframes conflict with any proposed new rules, the meaning and intention of the rules take precedence.

Wireframes

The wireframes in this document cover key areas of the ACCC's consultation paper, including:

4.1 Combined Accredited Persons
This allows an accredited outsourced service provider (CAP Provider) to collect CDR data from a Data Holder (DH) on behalf of an accredited data recipient (ADR), or 'CAP Principal' in this context.

4.2 Transfer of CDR data between accredited persons
This allows a consumer to consent to disclose CDR data from an ADR to another accredited person

5.1 Disclosure to trusted advisors
This allows a consumer to nominate a trusted advisor, including non-accredited persons, and consent to disclose their CDR data to that trusted advisor.

5.2 Disclosure of CDR insights
This permits ADRs to disclose an 'insight' derived from CDR data to any person, including non-accredited persons, with a consumer's consent.

7.1 Sharing CDR data on joint accounts
This allows a consumer to elect a disclosure option during the authorisation flow, plus additional messaging requirements for both joint account holders.

7.2 Amending Consents
This allows consumers to amend their consents on an ADR's dashboard, and allows ADRs to invite consumers to amend their consents.

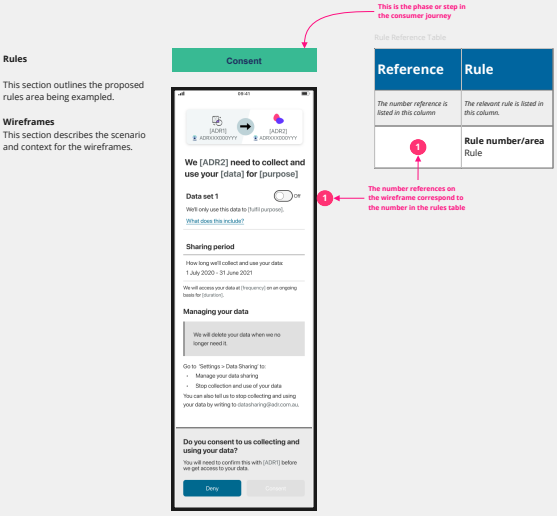
7.3 Separate Consents
This change separates collection and use consents, allowing different durations to occur for collection, use, and disclosure consents given to an ADR.

7.5 Data Holder Dashboard
These changes provide greater flexibility and consistency for the display of ADR details in the consent model.

7.7 Use of data for research
The proposed rules changes allow consumers to consent to ADRs using their CDR data for research purposes where it does not relate to the goods or services requested.

How to use

1.0 Each board is numbered and titled according to its section in the consultation paper



7.3 Separate Consents | 4.1 Combined Accredited Person

Rules: Separate Consents

The ACCC implemented a combined concept of a 'use and collection consent' in the current rules based on earlier consumer experience findings.

The ACCC is proposing to move away from this approach with the development of rules that allow for separate consents for collection of CDR data and consents to use CDR data.

Re-framing the rules so these consents are separate concepts creates more flexibility for accredited persons, and enables more granular consent options.

Example of the flexibility of separate consents
A consumer may have the following consents with an accredited person:

- Consent to collect for 24 hours;
- Consent to use for 3 months;
- Consent to direct marketing for 3 months;
- Consent to disclose to a trusted advisor on a single-occasion.

Given they are different consents, the consumer could independently withdraw or amend each consent.

Rules: Combined Accredited Persons

The ACCC has now made collection arrangement rules that expand the existing CDR outsourcing rules. This change will permit an accredited outsourced service provider (CAP Provider) to collect CDR data from a Data Holder (DH) on behalf of an accredited data recipient (ADR), or 'CAP Principal' in this context.

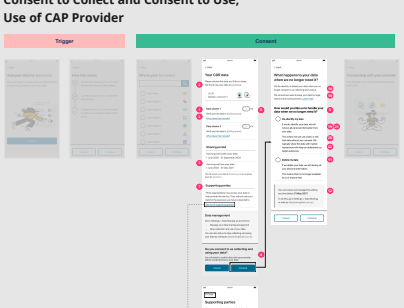
Wireframes

The scenario in this example outline how an ADR might collect data for one duration and use it for a different duration.

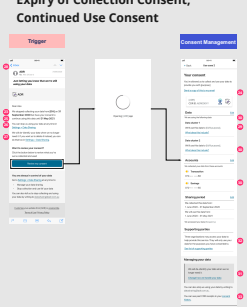
The ADR is also using a CAP Provider to collect data for this consent, along with non-accredited outsourced service providers to help deliver the service. The right to delete election pattern is shown to demonstrate how it may apply in this context.

The wireframes also provide an example of how, upon expiry of collection, an ADR may alert a consumer to an ongoing use consent.

Consent to Collect and Consent to Use; Use of CAP Provider



Expiry of Collection Consent; Continued Use Consent



Reference	Rule
	The relevant rule is detailed in the columns.
	4.11 Asking CDR consumer to give consent
4C	1) When asking a CDR consumer to give consent, an accredited person must: (a) allow the CDR consumer to choose the types of CDR data to which the consent will apply, and (b) allow the CDR consumer to choose the period over which the consent will apply, and (c) allow the CDR consumer to choose the period of the collection consent, and (d) allow the CDR consumer to choose the period of the use consent, and (e) not make the CDR consumer's choices in relation to the matters mentioned in paragraphs (a), (b) and (c) the default settings, and (f) allow the CDR consumer to withdraw authorisation to disclose CDR data in accordance with rule 4.26(1)(e).
4C	(i) in the case of a collection consent or a disclosure consent—the particular types of CDR data to which the consent will apply, and
4C	(ii) in the case of a use consent—the specific uses of collected data to which they are consenting; and
4C	(iii) allow the CDR consumer to choose the period of the collection consent, can only be for a period of one year or less, and is not to be a period that starts more than 90 days after the day on which the consent is given, and
4C	(iv) allow the CDR consumer to choose the period of the use consent, can only be: (A) on a single occasion; or (B) over a specified period of time; and
4C	(v) ask for the CDR consumer's express consent to the choices referred to in paragraphs (a), (b) and (iv) for each category of consents; and
4C	(vi) not present consents as pre-selected.
4C	(f) allow the CDR consumer to make an election in relation to deletion of redundant data in accordance with rule 4.16.
4C	2) The accredited person must not prioritise any given relevant options to the CDR consumer for the purposes of subrule (1).
4C	3) The accredited person must not make the election to delete redundant data in respect of the CDR data under rule 4.16.
4C	3) When asking a CDR consumer to give consent, the accredited person must give the CDR consumer the following information:
4C	(i) if the CDR data may be disclosed to, or collected by, an outsourced service provider—a statement to that effect and a link to the provider's CDR policy; and
4C	(ii) a statement that the consumer can obtain further information about such disclosure or collection if they wish; and
4C	(iii) a link to the accredited person's CDR policy; and
4C	(iv) a statement that the consumer can withdraw authorisation to disclose CDR data in accordance with rule 4.26(1)(e) and information about how to withdraw such authorisation; and
4C	(v) a statement regarding the CDR consumer's rights to elect that their redundant data be deleted; and
4C	(vi) instructions for how the election can be made;
4C	(i) if the CDR data may be, or will be, collected by the provider under a CAP arrangement—a statement to that effect; and
4C	(ii) the provider's name; and
4C	(iii) the provider's accreditation number; and
4C	(iv) a link to the provider's CDR policy; and
4C	(v) a statement that the CDR consumer can obtain further information about such collection or disclosure from the accredited person's CDR policy if desired.
	4.17 Information relating to redundant data
4C	1) For subparagraph 4.11(3)(f)(i), the accredited person must explain whether they: (a) will delete the redundant data when it becomes redundant data, or (b) will de-identify the redundant data; or (c) will do either, as the CDR data becomes redundant data, whether to delete it or de-identify it.
4C	2) An accredited person that gives the statement referred to in paragraph (1)(c) or (c) must, also state: (a) that, if it de-identifies the redundant data: (i) it would apply the CDR data de-identification process; and (ii) it would be able to use or, if applicable, disclose (by sale or otherwise) the de-identified redundant data without seeking further consent from the CDR consumer; and
4C	(b) what de-identification of CDR data in accordance with the CDR de-identification process means; and
4C	(c) if applicable, examples of how it could use the redundant data once de-identified.

Reference	Rule
	The relevant rule is detailed in the columns.
4C	**4.3 Request for accredited person to seek to collect CDR data** 1) A request that a CDR consumer gives a consent to collect CDR data is a request for the consumer to do one or more of the following: (a) an accredited person could continue to use CDR data it had already collected in order to provide the requested goods or services. However, the rectification requirement of rule 4.18A would apply
4C	**4.18 CDR receipts** 1) When an accredited person recipient gives the CDR consumer a notice that consents to collect, this is (a) a CDR receipt as soon as practicable after (a), the CDR consumer consents to given the accredited person to collect CDR data, or (b) the CDR consumer withdraws a consent or a voluntary notice or otherwise clearly indicates that they consent would apply; and, the CDR consumer amends such a consent in accordance with rule 4.12: (i) on a single occasion; or (ii) over a specified period of time; and
4C	2) Each for the CDR consumer's express consent to the choices referred to in paragraphs (a), (b) and (iv) for each category of consents; and
4C	3) Allows the CDR consumer to make an election in relation to deletion of redundant data in accordance with rule 4.16.
4C	4) The accredited person must not prioritise any given relevant options to the CDR consumer for the purposes of subrule (1).
4C	5) The accredited person must not make the election to delete redundant data in respect of the CDR data under rule 4.16.
4C	3) When asking a CDR consumer to give consent, the accredited person must give the CDR consumer the following information:
4C	(i) if the CDR data may be disclosed to, or collected by, an outsourced service provider—a statement to that effect and a link to the provider's CDR policy; and
4C	(ii) a statement that the consumer can obtain further information about such disclosure or collection if they wish; and
4C	(iii) a link to the accredited person's CDR policy; and
4C	(iv) a statement that the consumer can withdraw authorisation to disclose CDR data in accordance with rule 4.26(1)(e) and information about how to withdraw such authorisation; and
4C	(v) a statement regarding the CDR consumer's rights to elect that their redundant data be deleted; and
4C	(vi) instructions for how the election can be made;
4C	(i) if the CDR data may be, or will be, collected by the provider under a CAP arrangement—a statement to that effect; and
4C	(ii) the provider's name; and
4C	(iii) the provider's accreditation number; and
4C	(iv) a link to the provider's CDR policy; and
4C	(v) a statement that the CDR consumer can obtain further information about such collection or disclosure from the accredited person's CDR policy if desired.
	4.17 Information relating to redundant data
4C	1) For subparagraph 4.11(3)(f)(i), the accredited person must explain whether they: (a) will delete the redundant data when it becomes redundant data, or (b) will de-identify the redundant data; or (c) will do either, as the CDR data becomes redundant data, whether to delete it or de-identify it.
4C	2) An accredited person that gives the statement referred to in paragraph (1)(c) or (c) must, also state: (a) that, if it de-identifies the redundant data: (i) it would apply the CDR data de-identification process; and (ii) it would be able to use or, if applicable, disclose (by sale or otherwise) the de-identified redundant data without seeking further consent from the CDR consumer; and
4C	(b) what de-identification of CDR data in accordance with the CDR de-identification process means; and
4C	(c) if applicable, examples of how it could use the redundant data once de-identified.
4C	3) Details of each amendment that has been made to the consent.

4.2 Disclosure consent: ADR to ADR

Rules
Transfer of CDR data between accredited persons facilitates central CDR use cases, as well as encouraging competition and delivering convenience for consumers.

The proposed rules will permit accredited persons to collect and disclose CDR data between themselves in order to offer goods and services to consumers. The rules require a two-step process in order for the disclosure to be permissible:
1. The CDR consumer has a valid consent to collect and a consent to use in place with the accredited person (ADR 2)
2. The consumer has a valid consent to disclose in place with the accredited data recipient (ADR 1).

The transfers are not restricted to two accredited persons, and it may be that CDR data is transferred on to numerous ADRs, and then on to a non-accredited person.

The rules proposed in this section permit accredited persons to transfer CDR data between themselves in order to offer consumers distinct goods or services requested by consumers. For example, one accredited person could offer a product comparison service and then, with a consumer's consent, transfer CDR data to another accredited person in order for the consumer to acquire the recommended product.

Transfer between accredited persons may be initiated in two ways:
1. ADR 1 may recommend the good or service of ADR 2 to the consumer
2. the consumer may independently seek the good or service directly from ADR 2.

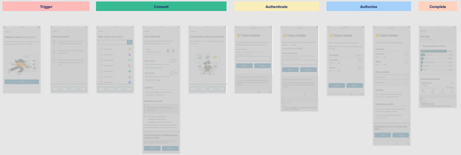
Where CDR data is transferred between accredited persons, each must independently provide consumer dashboards, CDR receipts and the appropriate notifications.

Wireframes
The wireframes provide an example use case where the ADR is providing a 'data wallet', where the consumer has shared their data to receive value added services.

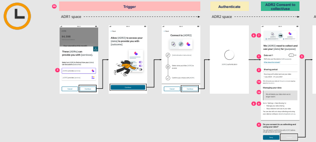
The consumer first gives the ADR a consent to collect and use their CDR data for the data wallet use case. Once this has occurred, the ADR provides them with the ability to disclose their data to various non-accredited persons for various value added services.

In this scenario, the initial value proposition occurs in the ADR (ADR1) space, and the consumer redirects to the other accredited person (ADR2) to get a collect and use consent, before redirecting back to ADR1 to give a disclosure consent. The consumer's subsequent interactions with ADR2 are assumed to occur separately.

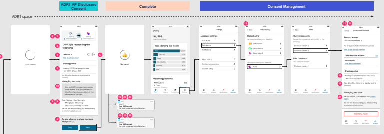
Original Consent



Disclosure Consent: ADR to ADR



Disclosure Consent: ADR to ADR | Dashboard



Reference	Rule
These reference numbers map to points in the wireframe/flow that illustrate how the proposed new rules could work in practice, but are not to be taken as compliant examples of these rules.	The relevant rule is listed in this column.
	4.7B Accredited data recipient may ask eligible CDR consumer for AP disclosure consent (3) If an accredited data recipient asks for an AP disclosure consent for the purposes of subrule (2), it must do so in accordance with Division 4.3.
	4.11 Asking CDR consumer to give consent (1) When asking a CDR consumer to give a consent, an accredited person must:
1	(a) allow the CDR consumer to choose the types of CDR data to which the consent will apply by enabling the CDR consumer to actively select or otherwise clearly indicate: (i) in the case of a collection consent or a disclosure consent—the particular types of CDR data to which the consent will apply; and
2	(b) allow the CDR consumer to choose the period of the collection consent, use consent, or disclosure consent (as appropriate) by enabling the CDR consumer to actively select or otherwise clearly indicate whether the consent would apply: (i) on a single occasion ; or (ii) over a specified period of time; and
3	(ba) in the case of a disclosure consent—allow the CDR consumer to select the person to whom the CDR data may be disclosed;
4	(c) ask for the CDR consumer's express consent: to the choices referred to in paragraphs (a), (b) and (ba) for each category of consents; and
5	(2) The accredited person must not present pre-selected options to the CDR consumer for the purposes of subrule (1).
	(3) When asking a CDR consumer to give consent, the accredited person must give the CDR consumer the following information:
6	(a) its name;
7	(b) its accreditation number;
	(g) the following information about withdrawal of consents:
8	(i) a statement that, at any time, the consent can be withdrawn;
9	(ii) instructions for how the consent can be withdrawn;
	(iii) a statement indicating the consequences (if any) to the CDR consumer if they withdraw the consent;
10	(h) the following information about redundant data: (i) a statement, in accordance with rule 4.17, regarding the accredited person's intended treatment of redundant data;
11	**1.14 Consumer dashboard—accredited person** (1) An accredited person must provide an online service that: (b) contains the details of each consent specified in subrule (3); and
12	(3) For paragraph (1)(b), the information is the following for each consent:
13	(e) if collection consent or disclosure consent applies over a period of time: (i) what that period is; and
14	(ii) how often data has been, and is expected to be, collected or disclosed over that period;
15	(ea) for an insight disclosure consent and a TA disclosure consent— to whom the CDR data was disclosed and when;
	4.18 CDR receipts (1) The accredited person must give the CDR consumer a notice that complies with this rule (a CDR receipt) as soon as practicable after:
16	(a) the CDR consumer consents to gives the accredited person a collection consent, a use consent or a disclosure consent; or
	(2) A CDR receipt given for the purposes of paragraph (1)(a) must set out:
17	(a) the details that relate to the consent that are listed in paragraphs 1.14(3)(a) to (f); and
18	(ba) in the case of a disclosure consent —the name of the person the CDR consumer has consented to the disclosure of CDR data to; and
19	(c) any other information the accredited person provided to the CDR consumer when obtaining the consent (see rule 4.11).
20	(4) A CDR receipt must be given in writing otherwise than through the CDR consumer's consumer dashboard.
21	(5) A copy of the CDR receipt may be included in the CDR consumer's consumer dashboard.
22	**4.19 Updating consumer dashboard** An accredited person must update a CDR consumer's consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.
23	**1.10C Trusted advisors** (1) An accredited person may invite a CDR consumer to nominate one or more persons as trusted advisors of the CDR consumer for the purposes of this section.

Reference	Consultation Paper reference	
These reference numbers map to points in the wireframe/flow that illustrate how the proposed new rules could work in practice, but are not to be taken as compliant examples of these rules.	The relevant paragraph is listed in this column.	Page this reference is found
25	**4.2. Transfer of CDR data between accredited persons** — Where CDR data is transferred between accredited persons and each accredited person is providing a good or service to the consumer, each must independently provide consumer dashboards, CDR receipts and the appropriate notifications.	page 26
26	**5. Greater flexibility for consumers to share their CDR data** — If an ADR offers this functionality, the proposed rules require the ADR to ask for the consumer's consent to disclose their CDR data to a non-accredited person separately from the initial consent to collect and use their CDR data.	page 29
27	— When asking for the consumer's consent to disclose to the non-accredited person, the ADR will need to comply with any standards made by the Data Standards Chair and have regard to CX guidelines made by the Data Standards Body. Any standards or guidelines may incorporate, for example, warnings that the non-accredited person may not be subject to the Privacy Act 1988 (Cth).	page 29

5.1 Disclosure to trusted advisors

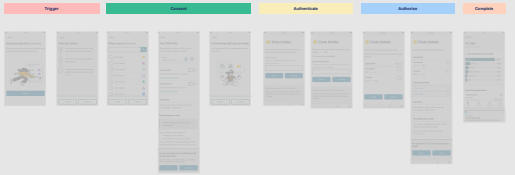
Rules
The proposed rules will permit ADRs to disclose CDR data to particular classes of non-accredited persons with a consumer's informed consent. The intent of these rules is to allow consumers the choice and flexibility to consent to an ADR disclosing their CDR data to their professional advisor so they can receive professional services in a manner that is convenient and secure, and avoid situations where the consumer may otherwise need to handle their data or share their credentials to provide access to their trusted professional.

Subject to the consumer's consent, the format and scope of the CDR data that an ADR could disclose to a trusted advisor is not limited. This raises a potential concern that an ADR could become a conduit for CDR data that enables other entities to receive CDR data without being accredited and attracting obligations under the CDR regime. The proposed rules seek to address this risk by only permitting disclosures by an ADR who are themselves supplying a good or service to the consumer.

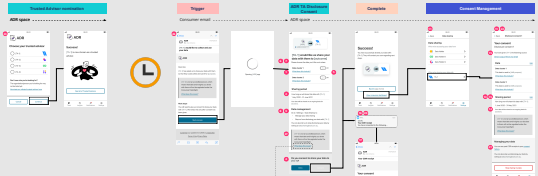
Effectiveness
The wireframes provide an agnostic ADR use case for the original consent, with the trusted advisor disclosure consent being presented after the original consent was established. This scenario assumes that the ADR provides the functionality for the consumer to nominate a trusted advisor, and that the ADR is responding to a request from the trusted advisor to access the consumer's CDR data on an ongoing basis.

In this scenario, the initial value proposition and disclosure consent occur in the ADR space, rather than being initiated in the trusted advisor's space, and the consumer's interactions with the trusted advisor occurring regarding.

Original consent



TA disclosure consent (ADR to Trusted Advisor)



5.2 Disclosure of CDR insights: ADR to non-accredited person

Rules
The proposed rules will permit ADRs to disclose an 'insight' derived from CDR data to any person with a consumer's consent. The intent of this rule is to recognise the broad range of services an ADR can provide both to consumers and third parties which, if provided with an 'insight', can be provided in a secure and safe way. This may include, for example, income and expense verification, verification of payments, or outcomes of responsible lending assessments.

The proposed rules do not seek to prescribe the specific kinds of products that are able to be offered. Instead, the proposed rules take a principled approach to defining an 'insight' as being derived CDR data that when disclosed is coupled with an identifier of the consumer, but taken without this identifier, could not reasonably be used to identify the individual consistent with the standard of de-identification set by the rules.

As drafted, 'insights' are derived CDR data. Therefore, they should not disclose any of 'raw' CDR data as originally disclosed by the data holder to the ADR.

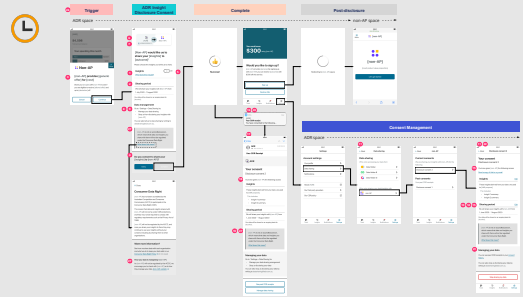
Wireframes
The wireframes provide an example use case where the ADR is providing a 'data wallet', where the consumer has shared their data to receive value-added services.

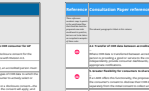
The consumer first gives the ADR a consent to collect and use their CDR data for the data wallet use case. Once this has occurred, the ADR provides them with the ability to disclose their data to various non-accredited persons for various value added services, including to access tailored offers.

In this scenario, the initial value proposition and insight disclosure occur in the ADR space, and the consumer only redirects to the non-accredited person if they choose to access the offer.

Original consent

Insight disclosure consent (ADR to non-Accredited person)





7.1 Sharing CDR data on joint accounts

Rules
The current rules do not permit consumers to set their preferences as part of the authorisation process. The proposed rules will require data holders to allow consumers to set their preferences as part of the authorisation process where consumers have not previously set up such preferences (for example, the first time the consumer initiates data sharing).

The proposed rules also detail requirements for the joint account management service provided by data holders and notification requirements, which align with current ACCC guidance, in light of feedback from CDR participants, the operation of joint account provisions is also intended to be simpler and clearer.

At this stage, the proposed rules do not require data holders to offer both 'pre-approval' (commonly referred to as 'one to authorise') and 'co-approval' (commonly referred to as 'two to authorise') disclosure options. Consistent with the approach under the current rules, the new rules propose that 'pre-approval' will be mandatory for data holders to offer, while 'co-approval' will be voluntary.

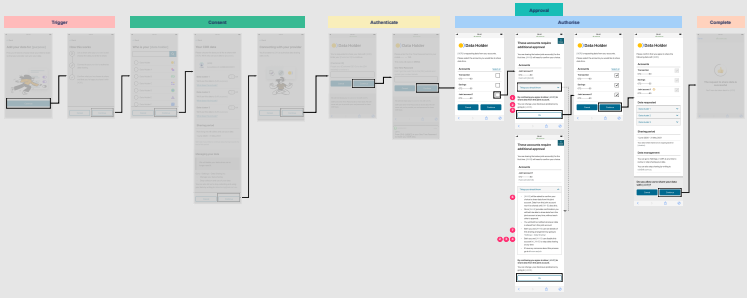
The proposed rules for amending consent and authentication also have implications for the joint account rules. The proposed rules are to the effect that regardless of which disclosure option is selected, if joint account holder A amends an authorisation, the data holder must notify joint account holder B of the nature of the amendment.

Joint account holder B will have transparency and high-level control over what CDR data can be shared by the data holder to an accredited person. It is not proposed, however, that joint account holder B will have oversight or control over further disclosure of CDR data by the accredited person. For example, if joint account holder A provides a consent CDR rules expansion amendments for an accredited person to disclose their CDR data to other persons, as contemplated in sections 5 and 4.2, joint account holder B will have no transparency or notification of that disclosure. This is because data holders do not have oversight of the consents or disclosures that occur after the initial disclosure.

Wireframes
These wireframes provide an example of how it might look when a consumer (account holder A) first chooses to share a joint account as part of the authorisation process, where the DH only provides a 'pre-approve' option. The second flow illustrates how additional notifications could be presented when account holder B is requested to approve a disclosure preference in their joint account management service.

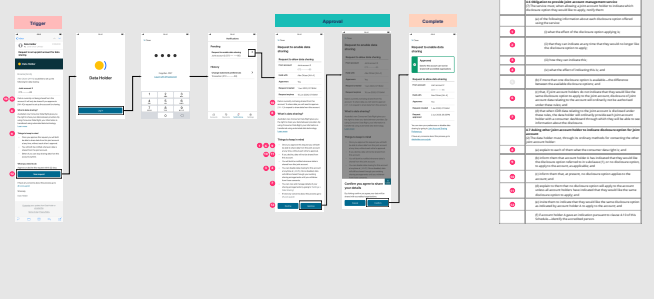
In-flow joint account disclosure option

Account holder A (AH-A)



Disclosure option approval

Account holder B (AH-B)



Reference	Rule
	Schedule 4—Provisions relevant to the banking sector
	4A Obligation to provide joint account management service
4A.1	The data holder must, when allowing a joint account holder to initiate which disclosure options may exist in a way, notify them:
A	(1) that the following information about each disclosure option offered and the following information about each disclosure option offered:
A	(1) what the effect of the disclosure option applying is
A	(2) that they can't indicate any time that they would no longer like the disclosure option to apply
A	(3) how they can indicate this
A	(4) what the effect of indicating this is; and
A	(5) if more than one disclosure option is available, the difference between the available disclosure options; and
B	(2) for a joint account holder, let the joint account that they cancel the same disclosure option to apply to the joint account, disclosure to joint account holder B will be stopped, and that they can't indicate this at any time that they would no longer like this to occur
B	(3) that when a joint account holder has indicated a disclosure preference (A) that when CDR data sharing to the joint account is disclosed under the pre-approval disclosure option, the other joint account holder will be notified with a consumer dashboard through which they will be able to see information about the disclosures
	4A.2 Joint account holders to indicate disclosure option for joint account
4A.2	(1) The data holder must, through its ordinary methods for conversing the other joint account holder:
A	(1) invite the joint account holder to indicate the consumer they prefer; and
A	(2) inform them that at any time they may indicate they would like the disclosure option referred to in subclause (1) or no disclosure option to apply to the account, as applicable; and
A	(3) inform them that, at present, no disclosure option applies to the account; and
A	(4) inform them that the no disclosure option will apply to the account unless all account holders have indicated that they would like the same disclosure option to apply; and
A	(5) invite them to indicate that they would like the same disclosure option to apply to the account as that which applies to the account; and
A	(6) if a disclosure option has been indicated by a person to whom subclause (5) invite—identify that accredited person

7.2 Amending consents | 7.7 Use of data for research

Rules

Under the current rules, in order to amend a consent, consumers must create a new consent consent or renew an existing consent and replace it with a new one. The proposed rules seek to expand the rules functionality, allowing consumers to have more control over their consents. This approach is consistent with the decision to increase functionality in the rules over time.

Amending consents could involve multiple attributes, including:

- adding or removing users
- adding or removing data types
- adding or removing accounts
- amending durations
- adding or removing data holders.

The proposed rules do not take a prescriptive approach and simply authorise amendments to consent. This means accredited persons are able to determine the best approach for their good or service. For example, some accredited persons may offer the ability to amend multiple attributes in one consent process, while others may not.

The proposed rules, also permit pre-selected options during the consent amendment process where the consumer has previously selected a particular option in the past.

This includes:

- data types
- time periods
- accredited persons (in the case of disclosure consents)
- data deletion elections

Given the separation of consents proposed at section 7.3 of this consultation document, as well as the ability to offer pre-selected options, we envisage the amendment processes will be streamlined, allowing the consumer to focus on the changing attribute.

Where consumers amend their consent, the proposed rules require the accredited person to notify the data holder, in order for the data holder to make the consumer to correspondingly amend their authorisation.

The proposed rules allow consumers to amend their consent through two mechanisms. Firstly, it is proposed that a consumer should be able to amend their consent at any time through the accredited person's consumer dashboard. Secondly, it is proposed that the accredited person should be required to offer the ability to amend some aspects of a consent. However, our current preference is that the accredited persons should be required to offer consumers the ability to amend the consent in the consumer dashboard to the extent possible, in order to encourage consumer control.

Secondly, it is proposed that accredited persons should be authorised to invite consumers to amend a current consent where the amendment would:

- better enable the accredited person to provide the requested goods or services to a consumer; or
- enable the accredited person to provide modified goods or services that have been agreed to by the consumer.

These limitations are proposed to ensure accredited persons are not 'spamming' consumers in order to seek additional data or uses.

Accredited persons may choose to offer multiple consent management options, such as amending consents, or withdrawing and replacing consents and concurrent consents as part of their service offering.

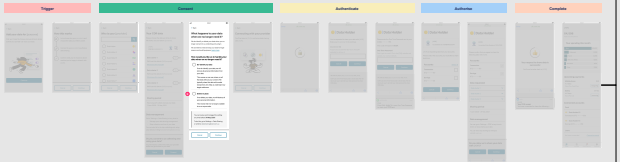
Wireframes

The following wireframes provide an example of how, after the original consent was established, an ADR may invite a consumer to amend their consent in a number of ways.

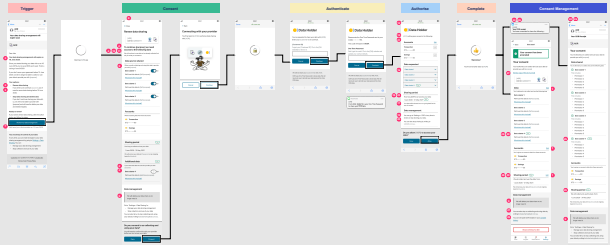
One flow incorporates an extension of the duration of an existing consent, and a proposed additional dataset for an enclosed value offering.

The other flow outlines how an ADR might invite a consumer to add users to an existing consent (a direct marketing use, and a general research use), noting that 'use' is enacted on the ADR side, meaning authentication may not be required in this scenario.

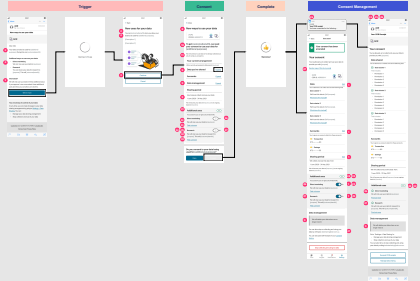
Original consent



Amending duration and data



Amending use | Use of data for research



7.5 Data Holder Dashboard

Rules
Under the current rules, data holders are required to present consumers with the name of the accredited person during the authorisation process and in the consumer dashboard.

The proposed rules ensure data holders are required to also display additional information to consumers that is held in the Register for the purpose of inclusion in the authorisation process or inclusion on the consumer dashboard. Additionally, the proposed rules ensure data holders are required to display additional information received through the data standards for the purpose of inclusion in the data holder's consumer dashboard.

Example of use case proposed rules are intended to support

Botanical is the parent company of Umbel.
Umbel offers consumers a tax-tracking app 'TaxCap'.
TaxCap requires concurrent consents to support its use case.

Under the current rules, 'Botanical', as the accredited entity, is required to be presented to consumers by data holders during the authorisation process and on the consumer dashboard.

The proposed rules require data holders to also display to consumers information entered by Umbel in the Register to also be presented during the authorisation process and on the consumer dashboard. For example, Umbel could require 'TaxCap by Umbel', or simply 'Umbel', to be presented during the authorisation process and on the consumer dashboard.

The proposed rules support data holders displaying to a consumer information as entered by Umbel in the metadata of certain data standards (for example, authorisation request metadata). This future functionality is intended to allow Umbel to have some 'free text' fields. For example, Umbel may use the free text to ensure the data holder displays their concurrent consent information in a meaningful way.

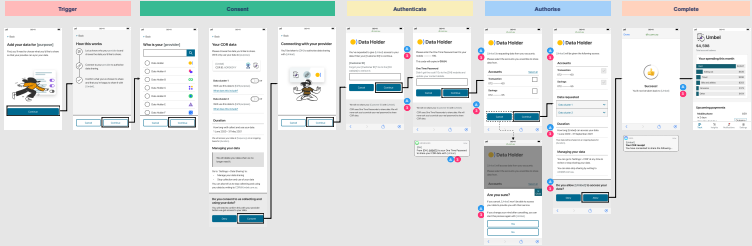
Wireframes and CX Considerations
This scenario provides an example of how the below (Fig.1) example ADR fields could display in the authentication and authorisation flows, as well as DH dashboards based on an array of possible dashboard designs.

The below fields are one example of what an ADR may choose to display in the consent model. It may be the case that some fields are equivalent to existing ones (e.g. the consent management field may be similar to the software product name), but allowing ADRs the choice of populating additional fields provides the flexibility to establish simple ADR structures, or more complex scenarios where multiple brands have multiple software products with concurrent consents.

To facilitate ADR presentation in the consent model, ADRs should receive a naming convention when registering software products and deciding the below fields, along with a UI demo to understand how their choices may appear in the consent model.

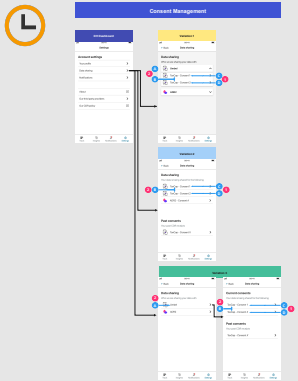
Field	Example	#
Legal Entity (ADR)	Botanical	
Brand	Umbel	
Field presented in authorisation flow for TaxCap App	Umbel	A
Field presented for consent management for TaxCap App	TaxCap	B
Field presented for 1st concurrent consent for TaxCap App	Consent 1	C
Field presented for 2nd concurrent consent for TaxCap App	Consent 2	D

Original Consent



Data Holder Dashboard: ADR Fields

Data Holder Dashboard | Design Variations for Example Fields (Figure 1.)



Reference	Rule
These reference numbers map to points on the consent journey that illustrate how the proposed text rules would be applied, but are not to be taken as compliant examples of those rules.	The relevant rule is listed in this column.
A	**1.15 Consumer dashboard—data holder** (1) If a data holder receives a consumer data request from an accredited person on behalf of a CDR consumer, the data holder must ensure that the CDR consumer has an online service to the CDR consumer that: (aa) contains any information in the data standards that is specified as information for the purposes of this rule; and
B	(bc) contains any information on the Register that is specified as information for the purposes of this rule; and
C	**4.23 Asking CDR consumer to give authorisation to disclose CDR data or inviting CDR consumer to amend a current authorisation** (1) When asking a CDR consumer to authorise the disclosure of CDR data or amend a current authorisation, a data holder must give the CDR consumer the following information about the authorisation or amendment: (ab subject to subrule(2)), the name of the accredited person that made the request;
D	(2) The data holder must also give the CDR consumer any information that the Register holds in relation to the accredited person that is identified as information for the purpose this rule.