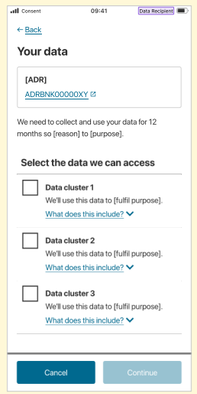
Consent review: Wireframes and proposed changes

NB: The visual examples below focus on screens that are relevant to the change proposals. To view the current consent flow in full, please refer to the CX Guidelines.

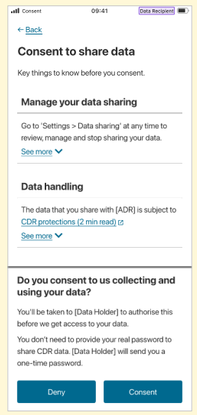
Current state example

Data



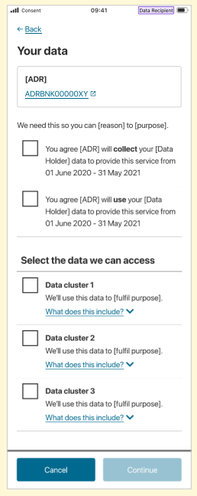
Access period

Consent to share data

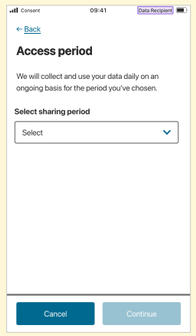


Variations

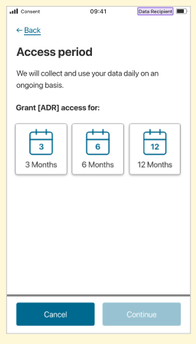
Data variation



Access period variation 1

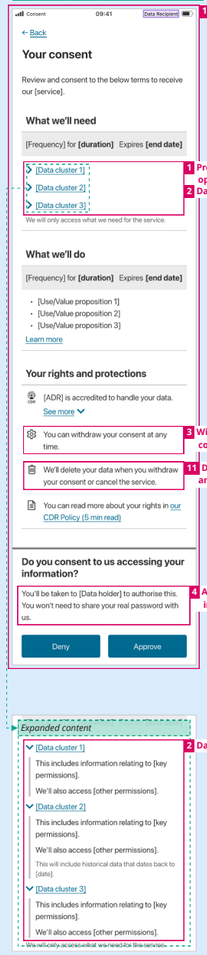


Access period variation 2



Proposed future state example

Data, Access period, Consent to share data



10 Separation of consents (bundling)

1 Pre-selected and actively selected options

2 Data language standards

3 Withdrawal of consent information

11 De-identification and Consent

4 Authentication information

2 Data language standards

Key Questions

- Do you agree with the preliminary proposals in this paper? If not, what changes or revisions should be considered?
- Do you agree with the initial scope of the consent review? If not, what might an alternative scope be, or what other changes should be considered as a priority?
- If the proposed changes were made, are there any implementation or consumer impacts that would need to be assessed?

Change Proposals - Complete List

Area	Details	Change Proposal
1 Pre-selected and actively selected options	**1 Pre-selected and actively selected options**	**1 Pre-selected and actively selected options**
Area Rule 4.11 require consumers to be able to actively select or otherwise clearly indicate datasets, uses and duration. Pre-selecting these is also prohibited; the rules suggest that un-filled checkboxes be presented to the consumer for selection. *(Noting Paper 273, page 5)*	***Details*** Active selection introduces false choice for consumers in scenarios where all the options are required for the service to function. CX research suggests that allowing consent to be provided for all essential and clearly indicated options at once can be done without negatively impacting informed consent. *(Noting Paper 273, page 5)*	***Change Proposal*** Clearly indicated options could be pre-selected if they are essential to the provision of the service. If certain options are not essential, the current active selection requirements could still apply. *(Noting Paper 273, page 5)*
2 Data language standards	**2 Data language standards**	**2 Data language standards**
Area Data Language Standards must be used to describe CDR data to consumers. This includes 'data cluster language' and 'permission language'. *(Noting Paper 273, page 5)*	***Details*** CX research suggests that describing permissions in a conversational way – rather than listing them as dot points – did not have a negative impact on comprehension or recall ability. *(Noting Paper 273, page 5)*	***Change Proposal*** The data language standards could be revised to make clear that ADRs and DHs can apply certain aspects of the data language standards more conversationally. *(Noting Paper 273, page 6)*
3 Withdrawal of consent information	**3 Withdrawal of consent information**	**3 Withdrawal of consent information**
Area Rule 4.11(3)(g) requires ADRs to provide consent withdrawal instructions and consequences when asking for consumer consent. *(Noting Paper 273, page 6)*	***Details*** CX research indicated that the absence of specific withdrawal details (instructions and consequences) did not negatively impact trustworthiness or informed consent. *(Noting Paper 273, page 6)*	***Change Proposal*** The requirements for withdrawal instructions and consequences to be displayed could be reviewed. These could be provided in the CDR Receipt. *(Noting Paper 273, page 6)*
4 Authentication information	**4 Authentication information**	**4 Authentication information**
Area The CX Authentication Standards require ADRs to clearly refer to the use of a "One Time Password" and state that consumer passwords aren't accessed for the purposes of CDR data sharing. *(Noting Paper 273, page 6)*	***Details*** Research to date has suggests that saying passwords will not be shared is viewed as sufficient, while specific references to 'One Time Password' (OTP) may be an unnecessary technical detail. *(Noting Paper 273, page 6)*	***Change Proposal*** The authentication standards could be amended so that ADRs no longer need to reference a 'One Time Password'. *(Noting Paper 273, page 7)*
5 Supporting parties	**5 Supporting parties**	**5 Supporting parties**
Area Rules 4.11(3)(f) and 4.11(3)(i) are inconsistent between the displaying of the names of sponsors, principals, and outsourced service providers (OSPs). *(Noting Paper 273, page 7)*	***Details*** CX research has consistently shown that being transparent about who may access the data is an important aspect of trustworthiness and informed consent. *(Noting Paper 273, page 7)*	***Change Proposal*** The various rules on displaying 'supporting parties' could be consolidated and simplified so they are consistent regardless of whether they are an OSP, principal, sponsor, or perform another role. *(Noting Paper 273, page 7)*
6 90-day notifications	**6 90-day notifications**	**6 90-day notifications**
Area Rule 4.20 requires ADRs to provide a notification to a consumer 90 days from the last time they accessed their dashboard. This is to remind them that a collection or a use consent is still current. *(Noting Paper 273, page 7)*	***Details*** Consumers may receive successive 90 day notifications for separate consents within similar time periods. CX research and heuristic analysis suggests that repeated notifications - particularly where the content is not tailored or actionable - may be unwelcome and lead to 'notification fatigue'. *(Noting Paper 273, page 7)*	***Change Proposal*** The rules could be amended to allow such notifications to be consolidated, made more actionable, and tailored according to consumer preferences. *(Noting Paper 273, page 7)*
7 Dark patterns	**7 Dark patterns**	**7 Dark patterns**
Area Removing prescription from the rules and standards provides greater implementation flexibility, but may leave the door open for 'dark patterns' to exist, which are intended to confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. Dark patterns have been explicitly considered and prohibited in various other jurisdictions, but have not been defined or prohibited in the context of CDR. *(Noting Paper 273, page 7)*	***Details*** CX Guidelines have explicitly avoided the use of dark patterns, but there are examples of dark patterns in live CDR implementations. *(Noting Paper 273, page 8)*	***Change Proposal*** A principle-based CX standard could be considered to prohibit interfaces, choice architecture, and design patterns that undermine, impair, or subvert user autonomy, choice, and decision making, and the CX Guidelines and other guidance could then provide relevant visual and theoretical examples to guide implementations. *(Noting Paper 273, page 8)*
8 Dashboards for once-off consents	**8 Dashboards for once-off consents**	**8 Dashboards for once-off consents**
Area Rule 1.14 and Privacy Safeguard 5 requires that ADRs provide a dashboard where consumers can review, manage and withdraw consent and authorisations. *(Noting Paper 273, page 8)*	***Details*** Preliminary CX research and heuristic analysis suggests that dashboards may not be necessary for consents where the data is collected once and not used for an ongoing period. *(Noting Paper 273, page 8)*	***Change Proposal*** The rules could be reviewed to assess if dashboards should be required for ADRs that only intend to support once-off consents with no ongoing use. (see also CDR receipts) *(Noting Paper 273, page 8)*
9 CDR receipts	**9 CDR receipts**	**9 CDR receipts**
Area Rule 4.18 require that ADRs provide a CDR receipt after a consent has been given, amended, or withdrawn. CDR receipts must include extensive details, including key elements of the consent and any other information provided to the consumer when obtaining the consent. *(Noting Paper 273, page 9)*	***Details*** CX research has highlighted the importance of the CDR receipt to maintain comprehension after consent has been granted while also serving as a record of what was agreed to. Certain information is better contextualised after consent has been provided, such as dashboard access and withdrawal instructions. *(Noting Paper 273, page 9)*	***Change Proposal*** The CDR receipt rules could be more explicit about what to include, and when to provide a CDR receipt. This could be refined to specify key and meaningful details; avoid extraneous information; and specify the inclusion of other information that may not currently be present or that may be removed from the consent flow to support simplification. *(Noting Paper 273, page 9)*
10 Separation of consents (bundling)	**10 Separation of consents (bundling)**	**10 Separation of consents (bundling)**
Area Rule 4.10 outlines the requirements for ADRs when seeking consent. It restricts the bundling of CDR consents with other directions, permissions, consents or agreements. For an ADR to provide services using CDR data, consumers would be required to provide multiple 'consents' to collect, use and/or disclose their CDR data. Separating CDR consents can result in more complex and duplicative consent flows. *(Noting Paper 273, page 9)*	***Details*** CX research has suggested that the duplication and complexity of consents for the one good or service may cause confusion and reduce comprehension and informed consent. *(Noting Paper 273, page 9)*	***Change Proposal*** The rules could be reviewed to allow 'bundling' of CDR consents for collection, use and/or disclosure consents where these consent types are necessary for the provision of the requested good or service. The consumer must still be presented with necessary information about the consents they are agreeing to. *(Noting Paper 273, page 9)*
11 De-identification and Consent	**2 De-identification and Consent**	**11 De-identification and Consent**
Area The CDR rules allow an ADR to de-identify consumers' CDR data in several ways, including where a consumer has provided a de-identification consent, or if the CDR data becomes redundant and a consumer has not elected that their data be deleted instead. Separate but similar requirements exist for each approach. *(Noting Paper 273, page 10)*	***Details*** Stakeholders have cited concerns and difficulties with the approach to de-identification in CDR. This includes that: • the rules on de-identification are complex and overlapping; • de-identifying consumer data is difficult to achieve in practice and, as such, may represent a risk to informed consent and consumer privacy CX research has shown a variety of consumer participant insights, including that: • they have a poor understanding of de-identification and the processes for electing that their data be deleted instead; and • they have a preference for their data to be deleted, as there was common belief that if their data was de-identified it could somehow be re-identified *(Noting Paper 273, page 10)*	***Change Proposal*** While we are not proposing specific changes at this time, community feedback is invited on the requirements and processes relating to de-identification and deletion in CDR, including if revisions should be considered. *(Noting Paper 273, page 10)*