SISS DATA SERVICES
OPEN BANKING API

Consumer Data Right:
Consultation on Combined Accreditation Process (CAP)

Submitted July 2020

About SISS Data Services

SISS Data Services (SDS) has been providing an open data solution as an Intermediary to FinTechs for ten years. SISS does not screen-scrape data. To deliver our service, we strongly believe in securely transferring only specific Consumer consented data to the specified SISS partner.

There are aggregators (who are possibly Intermediaries) that access Consumer data via screen scraping. These providers tend not to partner with Data Holders and have no accountability in the form of:

- Fine-grained consent to access only specific accounts
- Background checks of staff members
- Insurance
- Adhering to security best practices such as those required as part of CDR Accreditation
- Data Handling Policies and Procedures

There is another group of Intermediaries, such as SISS Data Services, who do partner with Data Holders and take their rights to access Consumer data very seriously. In this case, access to Consumer data is access directly from the Data Holder, following the Privacy Act. Data Holders only grant data access once the Intermediary has proven:

- They have a robust Consumer consent process (not screen scraping) which only allows access to specified accounts.
- Have undergone review(s) of their Security and their Policies and Procedures.
- Have systems and controls for the ongoing monitoring of their security.
- Provide Data Breach reporting to their Data Holder partners.
- Have contractual indemnity for data loss.

We refer to these Intermediaries as having a “direct data feed”.

More than 1 million accounts are accessed via direct data feeds[1]. SISS Data Services provides access to over 350,000 accounts via Direct Data Feeds.

[1] SISS Data Services, MYOB and Xero are the current Direct Data Feed users.

Current issues with the Consumer Data Right

The ACCC needs to address the following outstanding issues to ensure the introduction of the Combined Accreditation Process (CAP) achieves the desired outcome, if these issues are left unresolved, it will negatively impact the take up of the CDR by Consumers, ADR's and Intermediaries.

Access to CDR data by Addon or App partners

ADR's offer additional services and functionality to their Consumer via an eco-environment. The eco-environment consists of groups of Addon or App partners with a direct relationship with the ADR. At present the CDR Data Rules does not provide for an ADR to share data with an Addon or App partner, unless they hold an unrestricted level of accreditation which may not be commercially feasible for the Addon/App partner to attain. For context, 7 out of 10 of SISS Data Services' 450,000 direct data feeds connect to an Addon, App partner or third party.

An example of an Addon service is where a Consumer consents to share their CDR data from their Accounting Software Provider (the ADR) to an Addon that provides management reports to better manage their business.

Intermediaries' significantly reduce the compliance costs for ADR's and give them speed to market, however if an ADR is unable to share CDR data with their Addon/App partners, they are then unable to participate in the CDR regime, which ultimately disadvantages the Consumer for accessing secure consented data.

We believe this solution can be resolved by allowing an Addon to be classified as an outsourced provider where the Addon relates to providing services under the original consent, and introducing a lower level of accreditation where the Addon/App partner can only access data via an ADR, where the Consumer has provided consent.

Lower Tiers of Accreditation

Intermediaries provide a cost-effective pathway for ADR that do not need to access to the entire Open Banking data set, such as access to balance only data. The current accreditation process only provides for an unrestricted level.

Providing Data Back to the Consumer

There is an opportunity for the ACCC to extend the CAP arrangement to provide data back to the Consumer directly. SISS Data Services currently provides data back to Consumers directly. These Consumers tend to be large family offices or large businesses, but we also provide for FinTechs such as Digi.Me that provide Consumer storage options.

Our views on the CAP Arrangement

SISS Data Services is supportive of the proposed CAP Arrangement as outlined in the consultation paper dated 22 June 2020 and we believe that the proposals mostly provide for a stable framework for Intermediaries to participate in the CDR regime. There are some areas where SISS would like to see clarification.

Liability Framework

SISS Data Services agrees with the proposed liability framework.

Both SISS and our Customers (future ADR's) operate under a similar liability framework today with the major banks.

Minimum Information Security Controls

SISS Data Services agrees with the proposed minimum information security controls for Intermediaries under the CAP arrangement.

ACCC Registry

The role of the Provider validating the Principles accreditation with the ACCC Registry needs to be clarified by the ACCC.

Encryption in Transit

SISS Data Services support the safe and secure transfer of data with the CDR environment and this must also extend to the transfer of data between the Provider and the Principal under the CAP Arrangement.

Data Segregation

SISS Data Services has effectively and securely managed data for multiple recipients via logical separation for over 10 years. We believe physical separation of data is not required and would add additional and unnecessary costs to the Provider under the CAP arrangement.

Compliance Breach Reporting

We seek further information from the ACCC on how Compliance Breach Reporting will be managed under the CAP arrangement. Based on the proposed liability framework, SISS assumes all responsibility for compliance breach reporting resides with the Principal, even if the breach is a result of the actions of the Provider.

Activities Performed under CAP Arrangement

Care needs to be taken to ensure that existing security designs or proposed security designs do not severely restrict what services a Provider can offer to a Principal, for example:

In situations where the Principle and the Provider both perform activities on behalf of the Consumer, Providers need guidance on how this works practically with existing security controls. Both the Principle and Provider are registered ADRs.

As part of the CAP arrangement, are any components shared?

- SSA
- MTLS Certificates
- Product Registration

The two situations SISS are specifically interested in are:

Situation 1 – The Principle wants to control UX look and feel

- Fintech A is in a CAP arrangement with Provider 1 for Product Q.
- Fintech A has its infrastructure behind www.fintecha.com.au
- Provider 1 has its infrastructure behind www.provider1.com.au
- Data Holder Z has never been connected to by Product Q.
- Fintech A wishes to complete all consents with Data Holders but have Provider 1 do the collection of data when Fintech A requests it through the infrastructure supplied by Provider 1.

A Consumer wishes to connect Product Q of Fintech A to Data Holder Z.
At the start of the consent process, Fintech A uses Product Q to complete the Dynamic Registration with Data Holder Z, obtaining the required credentials.
The Consumer completes the consent, and Fintech A records the token.
Fintech A calls an API supplied by Provider 1 to update the registration details of Data Holder Z.
Fintech A then calls Provider 1, supplying the token, to obtain data.
Provider 1 makes the call to Data Holder Z with all the correct details.
Provider 1 routes the data back to Fintech A.

In Certificate Management of the CDR Register, it states that

Server Certificate(s)	Certificate is issued to a FQDN

Provider 1 should present which certificate - their certificate or the Principles certificate? Or is there a shared certificate? Or are both sets of infrastructures registered on the Principles certificate?

Situation 2 – The Principle will connect to some Data Holders directly, and use the Provider for others

- Fintech A has its registration for Product Q.
- Fintech A is also in a CAP arrangement with Provider 1 for Product Q.
- Fintech A wishes to connect directly with Data Holder Y for consent and data collection.
- Fintech A wishes to connect with all other Data Holders (including Data Holder Z) using Provider 1 for consent and data collection.
- Data Holder Y and Data Holder Z have never been connected to by Product Q.

A Consumer wishes to connect Product Q of Fintech A to Data Holder Z.
At the start of the consent process, Fintech A calls Provider 1 (supplying a Fintech A Unique ID for the Consumer),
Provider 1 uses Product Q to complete the Dynamic Registration with Data Holder Z, obtaining the required credentials.
The Consumer completes the consent, and Provider 1 records the token.
Fintech A then calls Provider 1 (supplying the Fintech A Unique ID for the Consumer), requesting Provider 1 obtain data from Data Holder Z.
Provider 1 makes the call to Data Holder Z with all the correct details.
Provider 1 routes the data back to Fintech A.

The Consumer now wishes to connect Product Q of Fintech A to Data Holder Y.
At the start of this consent process, Fintech A uses Product Q to complete the Dynamic Registration with Data Holder Y, obtaining the required credentials.
The Consumer completes the consent, and Fintech A records the token.
Fintech A then calls Data Holder Y with all the correct details to obtain the data.

Under the current proposed documentation, unless there is some variation on the Product Q name, the above scenario does not appear to be allowed.

Does Product Q get registered twice, once with the Principle as “Product Q”, and as part of the CAP arrangement against the Provider as “Product Q via Provider 1”? Or is there a shared registration?

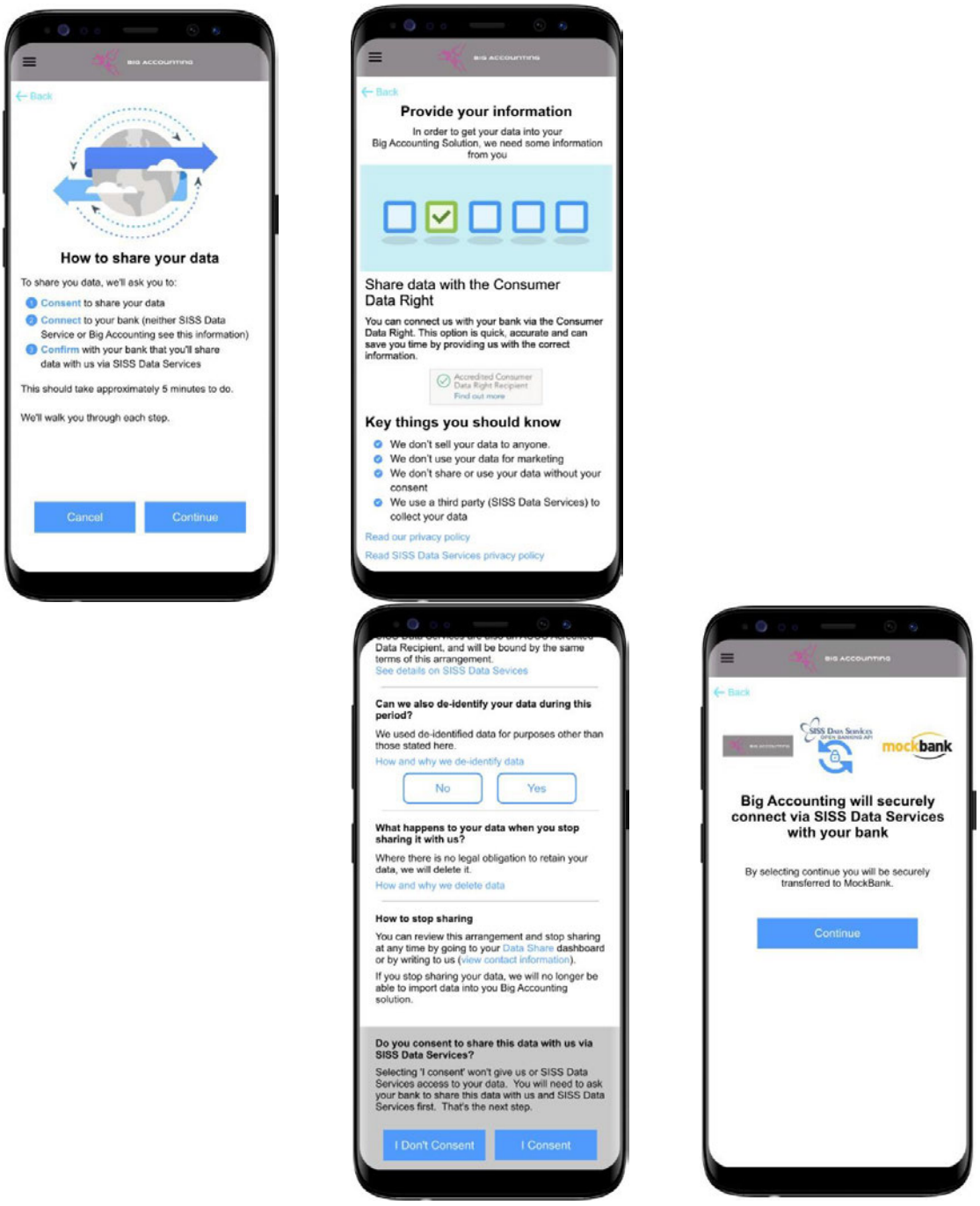
Disclosure of CAP Arrangement to a Consumer

For ADR using a CAP Arrangement Disclosure to the Consumer must be done when obtaining consent. Consent between the Data Holder and the ADR (Principal) and Provider should be transparent to the Consumer. To provide these visual cues, it can be as simple as including AIS information within the consent flow.

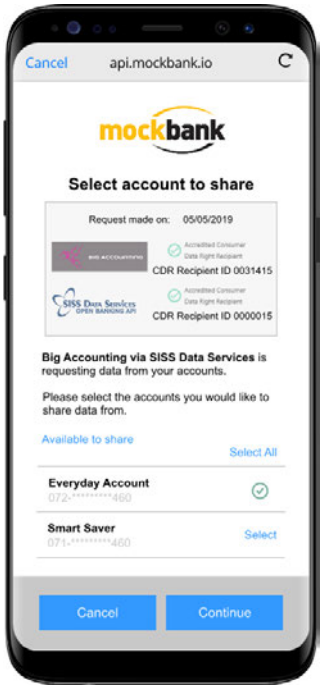
See SISS InVision CDR Consent Flow

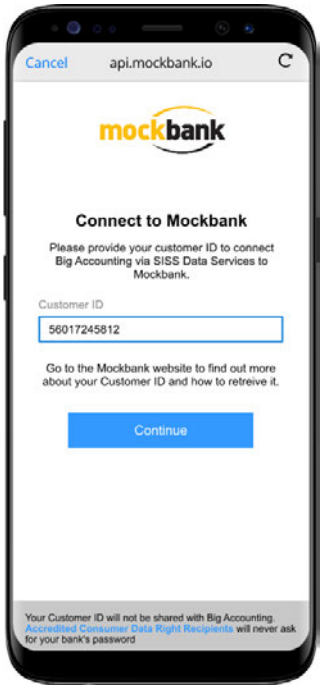
As a guiding principle, where CDR data is transferred or held outside of environments under the Data Recipients control, disclosure MUST be made in the consent process.

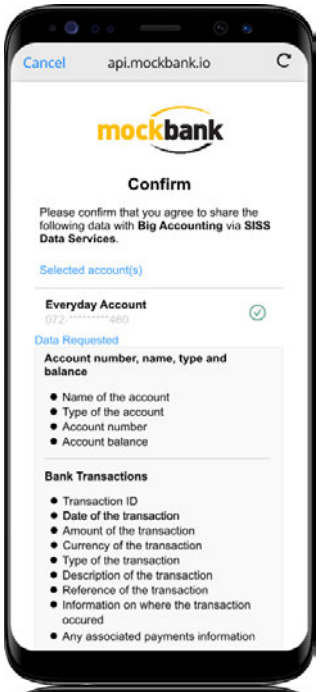
Data Recipient Consent screen when using a Provider

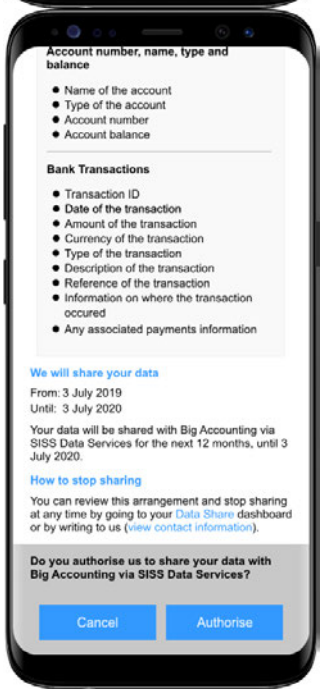


Data Holder Consent Screens with Provider included









SISS response to Privacy Impact Assessment

No.	Risk	SISS Response
1	Content of CAP Arrangements unclear The proposed amendments to the CDR Rules do not specify any mandatory provisions that must be included in CAP Arrangements.	SISS agrees that there should be a written and properly executed arrangement in place for a CAP. SISS also believes that there should be no prescribed format for this agreement. SISS would like to point out that the terms of a CAP may be included in a broader agreement between two parties.
2	Confusion over liability regime in CDR Rules, and which obligations apply to either the Principal ADR, the Provider ADR, or both	SISS agrees that there is some scope for confusion. However, we agree that as a combined unit both parties remain responsible with the principal being the primary point as they are the Consumer facing entity and the provider will primarily be backend technology solutions.
3	Information in Accredited Data Recipient Consumer Dashboard may not provide sufficient clarity to CDR Consumers	SISS believes the Dashboard should indicate the details of all parties to a CAP and endorse Maddocks recommendation of Provider ADR “X” will be used to collect CDR Data from Data Holder “Y”. SISS believes to maintain Consumer confidence & relationships the Primary ADR be included in the dashboard with the extra text (and accreditation numbers, links to websites) of the provider.
4	Security of the communication pathway between the Principal ADR and the Provider ADR for non-CDR Data about the CDR Consumer	SISS supports the recommendation that the transfer of CDR data be encrypted between the provider and principal. We do wish to note the requirements to participate in the CDR regime means utilising the published specifications, however the CAP does allow providers & principals to determine their own internal file specifications, communication protocols etc. Despite the freedom of using different standards internally it should not dilute the CDR requirement of data security.
5	Details of CDR Consumer’s consent and contact information not accurately transferred from Principal ADR to Provider ADR	SISS supports the recommendation that the transfer of CDR data be encrypted between the provider and principal.

No.	Risk	SISS Response
6	CDR Consumer unaware of to whom they are providing their consent	SISS acknowledges this risk is real and in reference to many comments in the Data61 CX interviews believes it is critical to keep the consent simple (and dashboards) and that the Principal ADR be the primary ADR displayed in the consent process. Branding, accreditation numbers, links to privacy policies etc will be for the principal ADR. Afterall, Consumers are likely to be initiating the consent workflow from the Principal ADR's app, website or software. SISS does acknowledge that the Provider should be mentioned, their accreditation number displayed, links to websites, privacy policy should be available to the Consumer but not in a way that clashes with the principal.
7	The Original CDR PIA report discusses the risks associated with the collection of the CDR Consumer's consent	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk
8	Technical information does not match the CDR Consumer's consent	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk
9	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient using the ACCC CDR ICT system	SISS acknowledges that the pathway between the ADR & ACCC could be compromised and that adding a new step or party in this pathway increases the security footprint. As ADR's SISS would suggest the various accreditation, regulation, reporting, auditing & legislative instruments are significant enough to ensure compliance by all parties (including Data Holders) in the CDR regime.
10	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient sending the Consumer data request to the Data Holder and redirecting the CDR Consumer Step 3 in the Original CDR PIA report),	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk. SISS agrees with Maddocks recommendation and wishes to point out that a standardised consent process for all ADR's & DH's across all industries leads to increased confidence in the CDR regime by Consumers.
11	Data Holder sends CDR Data to an Accredited Data Recipient that is no longer accredited	SISS agrees with Maddocks recommendations that the Data Holder should be required to check the credentials of both Principal and Provider before fulfilling a data collection request. SISS also suggests a requirement for Providers to check the credentials (status) of a Principal before providing data to the Principal. SISS recommends this in order to maintain confidence in the CDR regime. As there can be time gaps between the provider collecting data to when it is sent to the principal this requirement ensures only ADRs with proper accreditation are in receipt of CDR data.

No.	Risk	SISS Response
12	Misuse of Principal ADR's credentials by Provider ADR	SISS acknowledges this is a new risk in the CDR regime when considering the implementation of a CAP. As there is an arrangement between the principal and the provider this will be a legal matter covered by any legal agreement. As an ADR, providers have a vested interest in ensuring they maintain proper security standards and preventing the mis-use of credentials (as well as data and many other matters). Providers who are found to have mis-used credentials face losing their accreditation status.
13	The Original CDR PIA report discusses the risks associated with the CDR Consumer providing their authorisation to the Data Holder (see Step 4 in the Original CDR PIA report)	SISS doesn't believe this risk changes in regard to an CAP arrangement
14	The Original CDR PIA report discusses the risks associated with the Data Holder checking the credentials of the Accredited Data Recipient (see Step 5 in the Original CDR PIA report),	SISS doesn't believe this risk changes in regard to an CAP arrangement
15	The Original CDR PIA report discusses the risks associated with the Data Holder disclosing CDR Data to Accredited Data Recipient (see Step 6 in the Original CDR PIA report)	In reference to this risk, the recommendations from risk #11 also need to be considered in that Data Holders **and** Providers now have an obligation to not provide data to a non accredited person.
16	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient using CDR Data (see Step 7A in the Original CDR PIA report)	Under a CAP arrangement a Providers "purpose" for the collection of data is only to provide the CDR data to the Principal. In isolation a Provider has no purpose for the collection of data and as such SISS believes the Principal bears the primary responsibility for the proper collection of consent and use of the data. While SISS acknowledges a CAP joins two ADR's together and there is joint responsibility, we also wish to be clear around each parties role in the process.
17	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient disclosing CDR Data to its outsourced service providers (see Step 7C in the Original CDR PIA report)	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk
18	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient disclosing de- identified data to third parties (see Step 7D in the Original CDR PIA report)	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk

No.	Risk	SISS Response
19	The Original CDR PIA report discusses the risks associated with the Data Holder disclosing CDR Data to the Accredited Data Recipient (see Step 6 in the Original CDR PIA report)	SISS acknowledges some of the risks mentioned in Step 6, but doesn't believe a CAP solves or increases all the risk. With regard to the risk around Consumers visiting Dashboards we would like to re-iterate the importance that the Principal be the ADR listed. We believe a Provider ADR should not be included as this creates unnecessary friction and confusion, ultimately this could lead to Consumers withdrawing consent erroneously. SISS is comfortable with a requirement for the Principal ADR to mention and reference the Provider, rather than a separate listing on the dashboard.
20	Pathway security between the Provider ADR and the Principal ADR is compromised	In theory adding a new layer in the CDR data pathway does add a security risk. SISS agrees that both parties in the CAP need to be ADR's and comply with the associated requirements. SISS would like to point out that a key element of a Providers technology and business solution is risk management and mitigation, therefore we believe the security profile of a CAP could actually be stronger than ADR's not in a CAP arrangement.
21	Incorrect recipient of CDR Data	The risk of providing data to the wrong ADR or Consumer is already catered for in the rules. As an ADR a provider is required to meet these rules and risks the consequence (removal of accreditation) should an error occur.
22	Withdrawal or expiry of CDR Consumer's consent not communicated	SISS agrees with Maddocks that the communication of consent withdrawal is an issue for the parties within a CAP arrangement. SISS feels there is some value in modifying the rules but also points out if a consent has expired or been withdrawn, then when a data collection is attempted the Data Holder will not honor the request. Once a data holder invalidates the consent the risk of either party in CAP arrangement collecting data is removed.
23	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of the CDR Consumer's consent (see Step 8 in the Original CDR PIA report)	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk
24	Withdrawal or expiry of CDR Consumer's authorisation not communicated	As with issue 22, SISS agrees with Maddocks that the communication of consent withdrawal is an issue for the parties within a CAP arrangement. SISS feels there is some value in modifying the rules to ensure the combined unit (CAP) is required to notify the Data Holder of a withdrawn consent. We don't believe that there is such an issue with expired consents as all parties including the Data Holder should not be honoring an expired consent.

No.	Risk	SISS Response
25	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of the CDR Consumer's authorisation (see Step 9 in the Original CDR PIA report)	SISS acknowledges this risk but doesn't believe a CAP solves or increases this risk
26	Continued use of CDR Data by, or disclosure to, previously-accredited data recipient (either Principal ADR or Provider ADR), after accreditation ends	SISS agrees with the recommendations from Maddocks. While we hope ADR's don't lose their accreditation, it is a practical and a serious consideration, and it is also likely an ADR decides to no longer be accredited or the business ceases. SISS would also like to remind the ACCC that ADR's may be required to hold data to meet other legislative requirements (income tax, responsible lending, financial advice to a name a few) and as such any rule changes need to consider this.
27	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient's accreditation being suspended, revoked, or surrendered (see Step 10 in the Original CDR PIA report),	SISS agrees with the recommendations from Maddocks, relates to risk 26 above.
28	It is not entirely clear from the proposed amendments to the CDR Rules when a Principal ADR will be considered to have 'collected' CDR Data. That is, does the Principal ADR 'collect' the CDR Data when it is received by the Provider ADR or only when the Provider ADR provides the CDR Data to the Principal ADR.	SISS agrees with Maddocks this needs clarification. The view of SISS is there is a clear distinction that data collection by the Principal is when the Principal does actually get the data, and not when the Provider collects the data. This is why SISS believes that a Provider MUST be required to determine the status (via the ACCC registry) of a Principal before providing data to the Principal. In a similar vein Data Holders should be checking the status of both the Provider and Principal before honoring a data collection.