EnergyAustralia submission: Decision Proposal 225: Data Recipient Security Standards

As raised in previous responses to industry consultations relating to data security standards, EnergyAustralia still has concerns with the disclosure of sensitive customer data to entities where no *security-related data standards exist. As per the decision proposal 225 these entities include:*

- **Interface 3 (non-CDR):** Untrusted third-party apps connect to data holders using customer credentials
- **Interface 3b (non-CDR):** Connected third-party apps connect to first- and third-party apps
- **Interface 5 (CDR):** ADR collects CDR data from another ADR accredited
- **Interface 6 (CDR):** Sponsor and affiliate relationship
- **Interface 7 (CDR):** Unaccredited representative and principal relationship
- **Interface 8a/ 8b / 8c (CDR):** Trusted advisers

In summary, security standards should apply to any recipients receiving CDR data due to the sensitive nature of this data; ensuring an appropriate level of data security and privacy of the consumer is upheld as it flows beyond the boundaries of the data holder. Equivalent security standards should be applied between accredited data recipients and the non-accredited data recipients as in the above access arrangements.

#	Question	EA Response
1	What principles should the Data Standards Chair apply to determine if any security standards should be made for the CDR access arrangements?	*There are key principles which should be applied to all access arrangements to ensure customer trust and confidence as data flows beyond data holders. These principles are as follows:* • *Privacy* • *Identification, authentication & authorisation* • *Compliance and consent* • *Interoperability through secure integration* *Where possible, industry and/or global security standards must apply to all types of access arrangements including the NIST and security CIA triad of:* • *Confidentiality* • *Integrity* • *Availability* *We note that CDR data may contain personal information which is protected by the Privacy Act 1988 and the Australian Privacy Principles (APPs) contained in that Act. The APPs contain obligations to protect information from 'misuse', 'interference', 'loss' or 'unauthorised access'. While there are no prescribed data standards for misuse', 'interference', 'loss' or 'unauthorised access' of personal information, the protections are still established in the APPs. The APPs specify how personal information may be securely collected and used by entities.* *As such, consideration must also be given to the Office of Australian Information Commission's (OAIC) published guidelines on the Australian Privacy Principles (Australian Privacy Principles guidelines - Home (oaic.gov.au).* *And, as articulated in our previous EnergyAustralia submissions, consideration also needs to be made regarding how relationships and contracts with third parties are managed and comply with relevant standards.*

2	How should the Data Standards Chair determine whether standards apply to data recipient access arrangements, or not?	*CDR standards should be applied to all data recipient access arrangements; any time consumer data is being used or processed or accessed. (Consumer data is sensitive in nature and as such it is classified as confidential – therefore the principle of leveraging industry and global standards must apply) .* *Some classes of trusted advisor and data recipients might not have strong data security infrastructure or practices in place. This vulnerability highlights the need to meet broader regulatory requirements including the Privacy Principles that already apply to personal information (which CDR data may contain). We would suggest the best way to ensure this is to extend the data security standards to all data recipient access arrangements.*
3	If standards are supported, what standards are recommended, and why?	*All data standards must apply to all sharing and access arrangements to maintain customer trust and confidence as data flows between any and all entities. Compliance with CDR standards must be the minimum requirement. This is particularly relevant in the process of consent and the customer's ability to track where their data is and how it is being used/managed, including the ability to revoke access to data at any point in time.* *Scenarios which reduce the level of security and privacy create vulnerabilities, and opportunities for threat actors to take advantage of critical sources of personal information.*
4	What concerns or considerations must be factored into pre-existing commercial data integrations and solutions?	*Pre-existing commercial data integrations and solutions require special consideration; it is appropriate to review existing commercial arrangements and contracts to ensure that appropriate security contractual clauses are included and comply with the most up-to-date CDR standards and Australian Privacy Principles.* *This is of particular relevance where, as is the case with the Consumer Data Rights, that data standards are progressively being uplifted and updated to address increasing security threats and vulnerabilities.*
5	Are security considerations limited to any given sector or do they apply to all CDR data?	*Security should be considered for all sectors in which the CDR applies to ensure interoperability and customer trust; standards and principles should be defined and mandatory for all scenarios regarding the use of CDR data.*
6	Should the Data Standards define customer authentication requirements for customers authenticating with accredited persons or with non-accredited persons in a CDR access arrangement?	*In principle we consider that the data standards must define authentication requirements for customers authenticating with accredited persons and/or non-accredited persons in all CDR access arrangements. This will ensure the privacy and protection of CDR data. i.e. ensure that data is being disclosed at the request of the right person (e.g. the customer of the data holder).* *However, it is difficult to see how authentication will work if the accredited person or non-accredited person is authenticating the customer. The ability to initiate a One Time Password may be problematic in the event that the customer's number is not recorded or known; requiring an alternative means to verify the customer's identity. In relation to consent, the user experience of consenting to CDR sharing of data should be based on interoperability as well as notions of trust, integrity, and confidentiality as per the Privacy Safeguards. Consent and the ability to revoke consent must be bundled with consumer data as it is being shared and used. Data recipients should honour consent as delegated authorisation and comply with inherited responsibilities.*

7	If action initiation or payment initiation are introduced into the CDR, does this raise new or additional security considerations for access arrangements?	*If action initiation and payment initiation are introduced into the CDR, this raises new and additional security considerations for access arrangements.* *Action initiation and payment initiation are fundamentally different from the data sharing described in the current CDR requirements. Action or payment initiation would add complexity and require additional layers of security; we assume these initiations would be protected by the APRA standards, but additional CDR protections will also need to be considered.* *It is unclear and challenging to envisage how action initiation and payment initiation could extend to unaccredited parties. If this were possible, security considerations would need to be reviewed in light of the additional requirements.*
8	Are there any additional implementation or security considerations?	*There are 3 key additional implementation and security considerations. These include:* *a.* ***The cyber security threat landscape*** *is shifting and increasing in its complexity. In order to address this, the data standards are prescribing the implementation of FAPI 1 and subsequently FAPI 2 for CDR. Financial APIs such as FAPI1/FAPI2 are already being adopted internationally for the protection of personal information (not only financial data). The expectation is that CDR will be at the forefront of implementing international standards and capability particularly in light of the concerns associated with mismanagement of personal data.* *b. To reinforce EnergyAustralia's previous submission, "****Consent must be informed, unbundled and explicit".*** *In particular, informed consent should place an emphasis on informing the consumer when data is disclosed to an accredited person with restricted accreditation or outside the CDR regime. Strong consent is particularly necessary where there will be multiple consents and would be in place for potentially several accredited persons.* *We question the ability of customers to fully understand these multiple consents in tandem and the extent to which their data may be shared with further entities. We also have concerns that customers may be compelled to accept consents to receive the CDR goods or services from a non-accredited person."* *Consent must also be current to ensure that the relevant account holder or customer is providing the consent.* ***c. Ensuring that customers have transparency over disclosures of CDR data to non-accredited persons is key*** *to placing the customer at the centre of these decisions, in addition to strong consent frameworks. These disclosures are to trusted advisors and disclosure of insights to any person - outside the CDR ecosystem. (See prior submission by EnergyAustralia –17/2/22 Consumer Data Right Rules amendments – Version 3*