ADA ON CTRL

Assurance of Digital Assets (ADA) assessment of CTRL: a collaborative project of Australian Genomics and DNV

Final report

Report No.: 01, Rev. 01
Document No.: 01
Date: 30 March 2022

DNV Healthcare programme
Group Research and Development
Høvik 1363 Norway
Tel: +47 67 57 99 00

Project name:	ADA on CTRL
Report title:	Assurance of Digital Assets (ADA) assessment of CTRL: a collaborative project of Australian Genomics and DNV
Partner:	Australian Genomics
Partner contact:	Matilda Haas, matilda.haas@mcri.edu.au
Date of issue:	30 March 2022
Project No.:	10270630
Organisation unit:	DNV Healthcare programme GRD
Report No.:	01, Rev. 01
Document No.:	01

Applicable contract(s) governing the provision of this Report:

Objective:

Prepared by:	Verified by:	Approved by:
Sharm	MHaas	
Sharmini Alagaratnam Project manager, DNV	Matilda Haas Australian Genomics project liason lead	Anne Jorunn Stokka Principle researcher, DNV
Bobbie Ray-Sannerud Project team member, DNV		
Courtney Nadeau Project team member, DNV		

DNV Distribution:

☒ OPEN. Unrestricted distribution, internal and external.

☐ INTERNAL use only. Internal DNV document.

☐ CONFIDENTIAL. Distribution within DNV according to applicable contract.*

☐ SECRET. Authorized access only.

*Specify distribution:

Keywords:
Dynamic consent, digital assurance

Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by
0	2022-03-30	First issue			

Table of contents

Contents

1 EXECUTIVE SUMMARY

The widespread deployment of digital technologies across all facets of society challenges existing quality assurance and trust-producing mechanisms. As systems become more complex and interdisciplinary, they have the potential to impact a broader range of stakeholders, often in unforeseen ways. The Assurance of Digital Assets (ADA) framework developed by DNV is a flexible approach to assurance that takes into consideration the complexity of modern cyber-physical systems. ADA takes a holistic view that frames and analyses the ecosystem from a systems perspective, considering all elements of the system as whole and in its context. The framework gives a central role to the stakeholders and their diverse interests, goals, and concerns and is built on an iterative and goal-based assurance process. This process for assuring digital assets is split into two distinct stages: the first stage focuses on establishing an in-depth profile of the digital asset and its use, while the second stage focuses on substantiating claims by building and assessing knowledge in an assurance case.

CTRL is a web app operated by Australian Genomics that allows patients who have been offered genetic testing to record and update their consent preferences for participation in research projects. For CTRL to be successful, it must be trusted and accepted by participants in healthcare research, the public, and research organisations, where good governance for cross-jurisdictional information transfer is needed to facilitate research driven by large-scale data sharing. As a result of this awareness, DNV Group Research and Development (GRD), Healthcare programme aimed to test the value of and refine the ADA framework with CTRL as a use case. The overall goal was to further develop the ADA framework such that it supports the development of an assurance case for CTRL, by identifying and closing substantial trust gaps that may further support the successful implementation and scale of CTRL. As a result of common interests, a MOU to outline this collaboration was signed and the project was carried out from 17 Sept 2021 through 31 Dec 2021.

The project produced outputs under the two stages of the ADA framework. The Stage 1 outputs were an entity map, use cases for CTRL and findings from stakeholder interviews. These fed into a risk register, which was then structured into three main failure modes. In Stage 2, one failure mode was prioritized for the building of an assurance case, by collecting and structuring evidence to support claims about how CTRL manages the risks associated with this failure mode.

The results demonstrated utility in applying and providing a systems perspective on a healthcare technology, providing the owners a fuller overview of the system and where and how risk reduction actions could be taken and monitored. Examining CTRL’s layers of stakeholders and their interactions, building of the assurance case and substantiating claims all facilitate the closing of the trust gap to support the successful implementation and scaling of CTRL. Finally, this application of ADA on a healthcare use case demonstrates its value and utility in this sector.

2 INTRODUCTION

The Assurance for Digital Assets (ADA) on CTRL project ran through the date of agreement on 17 Sept 2021 through 31 Dec 2021. The project was a non-exclusive collaborative cooperation between DNV and Murdoch Children's Research Institute (MCRI) through Australian Genomics Health Alliance (Australian Genomics), to enhance the ability of DNV and Australian Genomics to jointly pursue and undertake opportunities to the mutual benefit of both. Australian Genomics is a network that brings together clinicians, diagnosticians, researchers, bioinformaticians, industry, policy makers and consumers who are united in their aim to achieve equitable and appropriate applications of genomics in healthcare. DNV is an independent assurance and risk management provider, operating in more than 100 countries, with the purpose of safeguarding life, property, and the environment. As a trusted voice for many of the world's most successful organizations, DNV helps to seize opportunities and tackle the risks arising from global transformations.

2.1 The ADA framework

The ADA framework (1) developed by DNV is an approach to close substantial trust gaps around digital assets introduced by the widespread deployment of digital technologies in all facets of society. In this project, CTRL, the dynamic consent-inspired solution developed by Australian Genomics, is considered as such a digital asset. The ADA framework is a generic guide to structure and establish assurance frameworks for diverse types of digital assets and their use in concrete industrial and societal contexts. It can be used to construct an assurance case, which is a logical chain of argumentation enabling a balanced view of supporting and contradicting evidence which are needed to support a scientifically sound substantiation of stakeholder claims. The ADA framework helps stakeholders and society at large to build an ecosystem of trust around their digital assets. It is designed to complement DNV's existing knowledge on assurance with new perspectives, methods and tools, and aims to be key in providing trust in the digital age. The ADA framework takes a holistic view that frames and analyses the ecosystem from a systems perspective, taking into account all elements of the system as whole and in its context. The framework gives a central role to the stakeholders and their diverse interests, goals and concerns and is built on an iterative and goal-based assurance process. This process for assuring digital assets is split into two distinct but intrinsically connected stages (see Fig. 1). The first stage focuses on establishing an in-depth profile of the digital asset and its use, while the second stage focuses on substantiating claims by building and assessing knowledge in an assurance case. A glossary of terms used in this framework is available in Section 6 at the end of this report.

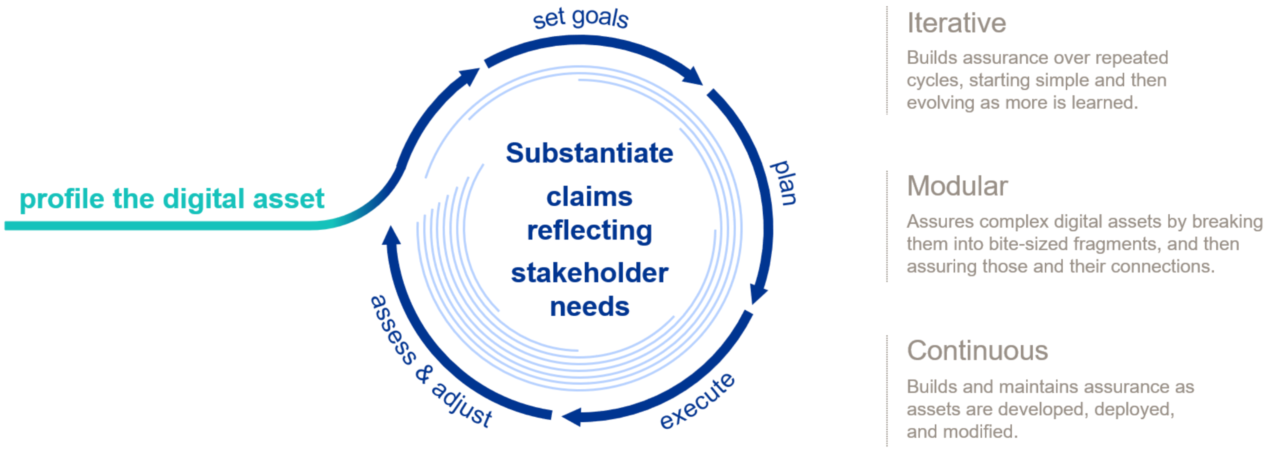

set goals
plan
execute
assess & adjust
profile the digital asset
Substantiate
claims
reflecting
stakeholder
needs
Iterative
Builds assurance over repeated cycles, starting simple and then evolving as more is learned.
Modular
Assures complex digital assets by breaking them into bite-sized fragments, and then assuring those and their connections.
Continuous
Builds and maintains assurance as assets are developed, deployed, and modified.

Figure 1. The ADA framework showing Stages 1 and 2, and its iterative, modular and continuous approach.

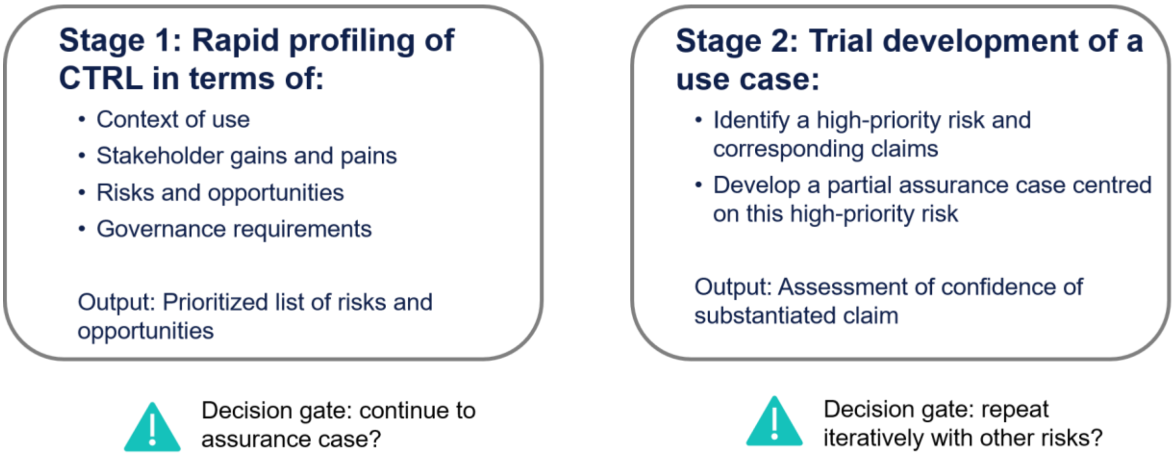
2.2 CTRL

CTRL was inspired by the concept of dynamic consent, and is a web app that allows patients who have received genetic testing to record and update their consent preferences for participation in research projects, for data sharing and for the return of incidental findings (2). The system was designed and developed by Australian Genomics with Curve Tomorrow and is administered and operated by Australian Genomics, leveraging infrastructure at its administering institution. CTRL incorporates educational aspects through embedded video and text supplied by Australian Genomics and study coordinators, and contains both messaging and notification functionalities. CTRL is integrated with a REDCap (Research Electronic Data Capture) clinical study database, also operated by MCRI, where changes to participant's consent preferences are registered. Both the CTRL system and the individual research studies are under the ethical oversight of the Royal Melbourne Human Research Ethics Committee.

CTRL's integration with REDCap and Metabase, a separate electronic data analysis tool, gives potential for integration with other systems like hospital electronic medical records (EMRs) and genomic data repositories. If multiple levels of integration can be achieved it will ensure that an individual's real-time choices are stored alongside their genomic or other health data, and data access will only be allowed with their permission.

2.3 Scope

The purpose of this project was to test and refine the utility of the ADA framework with a healthcare use case, namely the dynamic consent solution CTRL. The scope for this project was defined at the outset as the implementation of CTRL. The project consisted of two distinct stages with use of DNV's ADA framework as detailed in Section 2.1. As seen in Fig. 2 below, the first stage was applied to profile the dynamic consent software CTRL. The second stage developed an assurance case for one or more resulting identified risks as mutually agreed by the parties (see Section 6 for a glossary of terms used). The output of Stage 1 resulted in a list of risks and opportunities for CTRL which were prioritized by Australian Genomics and agreed upon for transition to Stage 2. Stage 2 output resulted in the development of an assurance case to assess the confidence in the top-prioritized claim.



Stage 1: Rapid profiling of CTRL in terms of:

- Context of use
- Stakeholder gains and pains
- Risks and opportunities
- Governance requirements

Output: Prioritized list of risks and opportunities

Decision gate: continue to assurance case?

Stage 2: Trial development of a use case:

- Identify a high-priority risk and corresponding claims
- Develop a partial assurance case centred on this high-priority risk

Output: Assessment of confidence of substantiated claim

Decision gate: repeat iteratively with other risks?

Figure 2. The ADA framework applied to CTRL: Stages and decision gates.

In order to accomplish this, DNV made available personnel and other required resources to complete both deliverables, of which included researchers with backgrounds in standardization, cyber security, human factors, software development, bioinformatics, assurance and risk assessment. Australian Genomics provided relevant documentation and access to relevant stakeholders with knowledge of CTRL to facilitate these explorations. The project consisted of the following major activities detailed in Table 1.

Table 1. Timeline listing significant activities carried out in the project by partners.

Date	Activity	Participants
Sept 17, 2021	MOU and project agreement signed	DNV, Australian Genomics
Sept 21, 2021	Project kick-off	DNV, Australian Genomics
Sept 22, 2021	Gather and submit CTRL documentation	Australian Genomics
Sept 23-Oct 7, 2021	Document review	DNV (competencies in bioinformatics, cyber security, human factors, data science, and risk management)
Sept 23 – Oct 18, 2021	Stakeholder interviews	Interviewees: CEO of an Australian rare disease patient organization, Data Officer of Australian Genomics, Data Manager of Australian Genomics, two Genetic Counsellors, National Coordinator for a clinical genomics study, Human Research Ethics Committee, two CTRL product owners, senior hospital administrator
Oct 19, 2021	Review of draft entity map	Australian Genomics
Oct 7-19, 2021	Development of risk register	DNV
Oct 21, 2021	ADA on CTRL Risks and Opportunities workshop	DNV, Australian Genomics
Oct 28, 2021	Prioritization of risks for transition to ADA stage II	Australian Genomics submitted selection via email with document as safeguards against data breach
Oct 30-Nov 10, 2021	Development of claims and assurance strategy for data breach risks	DNV
Dec 2, 2021	Workshop on assurance case methodology	DNV, Australian Genomics
Dec 13, 2021	Conclude next steps	DNV, Australian Genomics
Dec 17, 2021	Final report submitted	DNV, Australian Genomics

2.4 Project motivation

The concept of dynamic consent was developed with the primary purpose of improving participant choice and engagement in research, but by its design also offers a range of potential advantages to research organizations, and its model is still evolving. The Australian Government’s National Genomics Policy Framework Implementation Plan (2018) specifically includes an action to “consider the role of consent models for health care and data-sharing purposes, including… dynamic consent.” Australian Genomics has been among the first globally to research and pilot the dynamic consent approach and its application to genomic studies. The first phase of development of the CTRL platform was completed and launched in December 2018, and received ethical approval to run a pilot study to compare the use of CTRL with standard paper-based consent. The value of CTRL is that by registering for the website, participants can revisit study information and make changes to their consent choices at any time. By being involved in CTRL, participants can also be kept better informed on their progress through the study, as well as receiving further health information and updates on study outcomes.

Interest in this project stems from the awareness that for CTRL to be successfully implemented it must be trusted and accepted on at least three levels, 1) by participants in healthcare research, and the public, 2) by research organizations, and 3) between research organizations, where good governance for cross-jurisdictional information transfer is needed to facilitate research driven by large-scale data sharing. As a result of this awareness, DNV Group Research and Development (GRD), Healthcare programme aimed to test its value and refine the ADA framework with CTRL as a use case. The overall goal was to further develop the ADA framework such that it supports the development of an assurance case for CTRL by identifying and closing substantial trust gaps, and further support the successful implementation and scaling of CTRL. Currently, the ADA framework is a generic guide to structure and establish assurance frameworks for diverse types of digital assets and their use in concrete industrial and societal contexts. As a result of common interests, an MOU to outline this collaboration was signed and the project run from 17 Sept 2021 through 31 Dec 2021. The outputs from Stage 1 and 2 are detailed below in section 3.

3 STAGE 1: PROFILING OF CTRL

3.1 Introduction to Stage 1

The initial profiling stage of the ADA framework is made up of several steps, each with a series of activities that lead to a full understanding of the asset and its intended use, as shown in Fig. 3. The profiling stage aims to produce several specific output items that are key inputs to the assurance case in Stage 2 to build the necessary trust and confidence in the asset and its use.

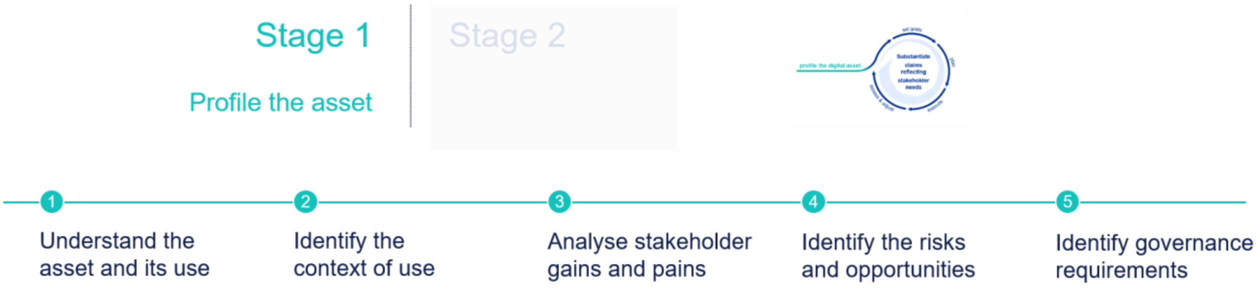

Stage 1
Profile the asset
Stage 2
profile the digital asset
Substantiate claims reflecting stakeholder needs
1
Understand the asset and its use
2
Identify the context of use
3
Analyse stakeholder gains and pains
4
Identify the risks and opportunities
5
Identify governance requirements

Figure 3. The individual activities undertaken in ADA Stage 1 to profile CTRL.

In this project, the Stage 1 profiling of CTRL was performed in five steps based roughly on Fig. 3, specifically: 1) identifying the context of use; 2) analyzing the stakeholders and their needs and concerns; 3) identifying system-related opportunities and targets, losses and hazards; 4) identifying governance requirements; and 5) consolidating the output of the profiling stage.

3.2 Context of use

Step 1 began with the review of the following documents provided by CTRL to DNV, consisting of a 2.3 GB repository of documents detailing the design, implementation, governance, technical requirements and other aspects of CTRL. The review of documents leveraged competencies from DNV within bioinformatics, cyber security, human factors, data science and risk management. Documents were sorted by content and reviewed, and key aspects about CTRL were summarized.

This document review, together with the stakeholder interviews described in 3.3, allowed the context of use for CTRL to be identified. CTRL is a software inspired by dynamic consent, and is designed and implemented by the Australian Genomics. Software development was sub-contracted to Curve Tomorrow, an Australian software house, and the local implementation on MCRI infrastructure is managed by MCRI IT teams. To date, the software is used by participants who have been offered genetic testing as part of their participation in Human Research Ethics Committee (HREC)-approved clinical studies to manage their consent preferences regarding data sharing, return of incidental findings, and contact regarding future participation in research projects. As part of the clinical workflow for these research participants, CTRL serves several core functions supporting these studies. Firstly, CTRL serves as a mechanism for two-way communication, and provides participants vital information about genetic testing through its in-built education and blog functions. Secondly, by allowing research participants to change their consent preferences, CTRL supports participant engagement and empowers participants to control access to their own health data. Finally, CTRL serves an important governance role by supporting transparency and two-way communication between the researchers and participants.

CTRL is comprised of a PostgreSQL database and a participant-facing web app, built with Ruby on Rails. Access through this web interface is password controlled, and access via MCRI is controlled through their standard security practices. In addition to CTRL and REDCap, the CTRL database can be monitored through Metabase, an SQL business intelligence dashboard also installed on MCRI servers.

The CTRL database is integrated with the Australian Genomics REDCap database. REDCap is a commonly used secure, web-based application for data capture in research studies (3). The Australian Genomics REDCap database contains various fields for health data depending on the study in question, including personal contact details, demographics, clinical information, genotypes, pathology results, survey responses, study logistics and tracking information, and consent preferences pushed from the CTRL app via an API. For de-identification, participants are assigned a unique Australian Genomics study identifier, generated in REDCap.

Both REDCap and CTRL are hosted on a secure server at MCRI, supported by a dedicated IT team. Physical and cybersecurity is managed by teams within MCRI. MCRI have processes in place to control physical access to servers including local security, video monitoring, and card-controlled access to server rooms. A third-party security provider conducts penetration testing biannually. Access to MCRI systems is controlled through standard security practices including password protection and user access rights segmentation. Cybersecurity is actively managed to identify and protect against attacks, and servers and databases are backed up nightly.

3.2.1 Entity map

A visualization was developed to help summarize the understanding of CTRL and its context of use. The CTRL entity map shown in Fig. 4 was generated from the various stakeholders and systems identified during this document review (described in 3.1.1) and further refined by review with Australian Genomics. The map included any organizations, systems or individuals that interact with CTRL, including the actions they perform with the system and their specific use cases for CTRL. Direct and indirect interactions between entities were noted, along with specifics about how these interactions occurred.

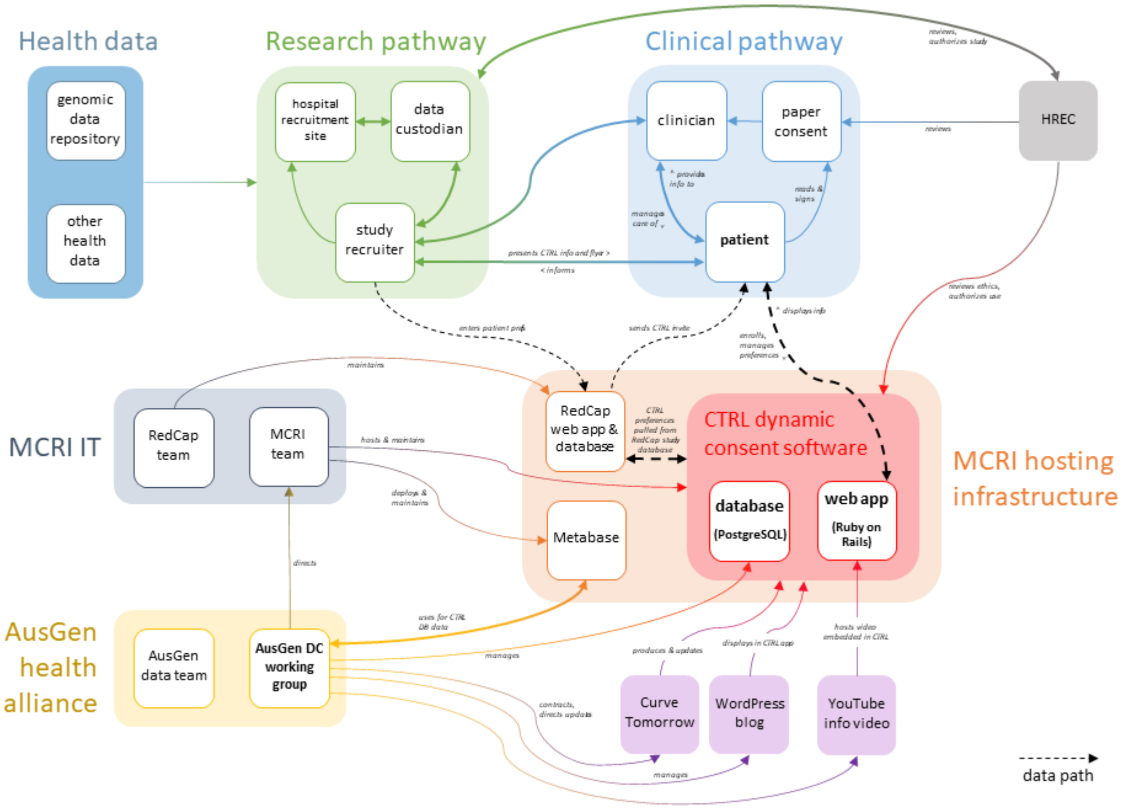


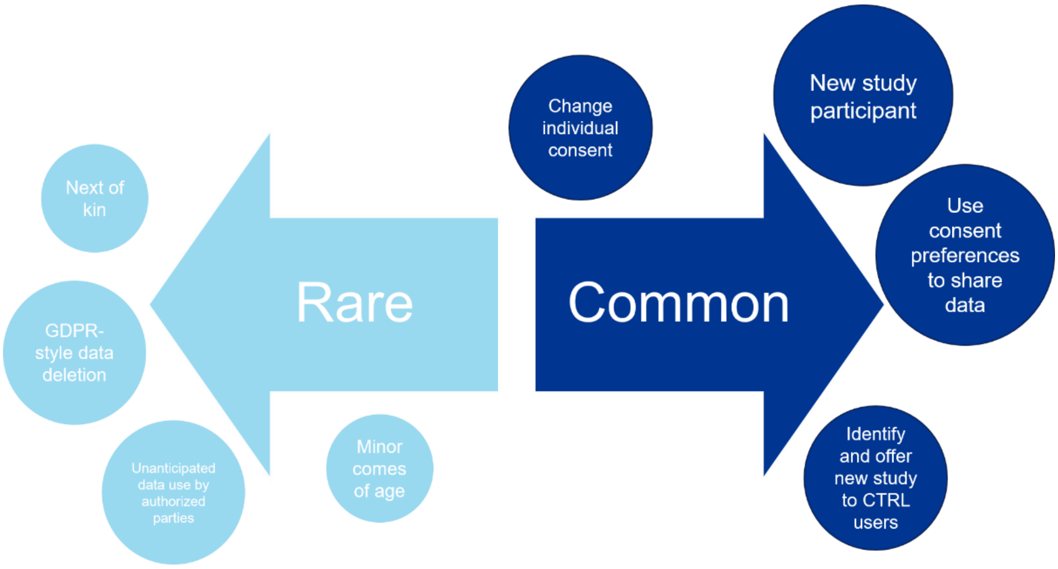
Figure 4. The entity map showing organizations, systems or individuals that interact with CTRL, including the actions they perform with the system, their use cases and direct and indirect interactions with CTRL.

3.2.2 Governance requirements

Stage 1 included the identification of relevant governance requirements. Due to CTRL's handling of personal sensitive data, the Australian *Privacy Act 1988* was identified as most relevant for understanding as it regulates how organizations collect and handle personal information, including health information. It also includes provisions that generally allow an individual to access information held about them. Guidelines under Section 95 of the *Privacy Act 1988* set out procedures that HRECs and researchers must follow when personal information is disclosed from a Commonwealth agency for medical research purposes. The *Privacy Act 1988* contains 13 privacy principles which gives an organization or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies. A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

3.2.3 Use cases

When data flows were mapped onto the entity map, it became apparent that several possible workflows existed using CTRL in this context, ranging from very common to very rare. These workflows are shown in Fig. 5 below, and detailed in Table 2.



Next of kin
GDPR-style data deletion
Unanticipated data use by authorized parties
Minor comes of age
Rare
Change individual consent
Common
New study participant
Use consent preferences to share data
Identify and offer new study to CTRL users

Figure 5. Identified workflows for CTRL mapped according to how rarely or commonly these are employed.

Table 2. Description of workflows identified for CTRL ranked according to how commonly or rarely they are employed.

Occurrence	Workflow	Description
Most common	New study participant	The most common workflow, which CTRL has been primarily designed around. In this instance, a research study participant who has been enrolled via REDCap has agreed to manage their consent preferences via CTRL. They receive an automated email, create a CTRL account, review educational materials, and set their initial consent preferences. In the back-end, data from CTRL is mirrored to REDCap, and Australian Genomics staff perform data quality checks both manually and via Metabase.
Common	Change individual consent	From stakeholder interviews, this is not the most common workflow but will presumably increase with broader adoption of CTRL. In this workflow, a participant with an existing CTRL account logs in via the website, changes one or more consent preferences, and logs out. These changes are then flagged to the Australian Genomics team and propagated to REDCap via API, and should lead to changes in the management of this participant's data (for example, by opting out of contact regarding future studies).
Common	Use of consent preferences to share data	In this workflow, researchers conducting a clinical study refer to consent preferences held in the CTRL databases to inform their decisions about how to manage a participant's data. After reviewing preferences, researchers use this information to inform their actions such as granting data access, contacting the participant regarding new studies, or providing information to the participant.
Rare	Minor participant in CTRL becomes of age	In some cases, the legal guardians of a minor research participant may create an account in CTRL and manage consent on behalf of the participant. When the research participant comes of legal age, this workflow is needed to effectuate the transfer of responsibility from the guardian to the participant.
Rare	Participant dies: next of kin workflow	In the event that a research participant passes away, this workflow describes the systems and procedures in place to manage the participant's data after their death, such as transferring account ownership, deleting accounts, and informing next of kin about the account.
Very Rare	Participant requests account deletion or data	This workflow describes situations when a research participant requests a copy of their data (through GDPR or similar) or when a research participant requests the deletion of their account and any personal data held by Australian Genomics.
Very Rare	Unauthorized data access	In the event that data in CTRL is breached, stakeholders in MCRI and Australian Genomics perform various tasks to investigate the breach, contact participants, restore data, and confirm the integrity of systems in the MCRI infrastructure.
Very Rare	Unanticipated data use by authorized parties	In this workflow, Australian Genomics becomes aware of a data breach or of unauthorized data use at a partner institution that has been granted access to data on the basis of consent preferences held in CTRL.

3.3 Stakeholder Interviews

To build a better understanding of the stakeholders which interact with and are impacted by CTRL, DNV conducted a series of interviews at which Australian Genomics participated as observers. Semi-structured interviews were administered to a total of 9 identified stakeholders meant to represent a broad set of the organizations impacted by CTRL, as identified during entity mapping. The interview format included questions on how they interact with CTRL, the requirements for trust that they and their organizations have, the realized and potential benefits CTRL provides, the risks and potential negative consequences they could face due to CTRL, and the opportunities that CTRL delivers. A summary of the stakeholders and their respective findings are described below.

1) The CEO of an Australian rare disease patient organization, whose members often receive genetic testing and may participate in clinical research.

    a. Patients are generally willing to share data, but wary of commercial use.
    b. No substantial difference between willingness to share data for research versus for treatment of other patients.
    c. Key issues are commercial use of data, and vulnerability of patients who are thrust into this situation.
    d. Dynamic consent important due to information overload at start of genetic testing.
    e. Biggest concern is how to implement claw-back of consent and data. Expectation setting critical.
    f. Patients generally more concerned about inappropriate sharing than data security. Also concerned about insurance implications.
    g. Availability of dynamic consent, whether used or not, increases trust.

2) The Data Officer of Australian Genomics, who actively monitors CTRL, sets up database analytics and has a role in managing data quality.

    a. CTRL saves team time and effort versus paper consent.
    b. Concerned about technical issues, but many checks and balances in place to identify those early. Actions often manual or semi-automated.
    c. Infrequent user interactions and current scope mean availability not a key issue versus confidentiality and integrity.
    d. Low activity users, also due to the type of system it is. Value in existing, whether or not people use it.

3) The Australian Genomics Data Manager, who has a role in managing data and data repositories for clinical studies, including data for which access is controlled via CTRL.

    a. Various data systems in use need coordinating, systems to help them manage governance.
    b. Granularity of choice leads to increased trust in system.
    c. Behind the scenes lots of manual checks before data sharing.
    d. Participants need to understand limitations to claw-back data. Setting expectations.
    e. Delegated trust from patients to data managers.
    f. Is informed consent really informed? CTRL-specific: do participants share same understanding as Australian Genomics?
    g. Sustainability of CTRL versus the data repositories might undermine trust in research system.
    h. Federated data processing might be a catalyst for wider dynamic consent use.
    i. Pain points due to mismatch between dynamic consent and traditional paper. May undermine longevity of datasets.
    j. Spends a lot of time manually and semi-automatically generating cohorts, data access reviews.

4) Two Genetic Counsellors who have primary roles in patient treatment and in recommending or enrolling patients in clinical studies, sometimes via CTRL, where appropriate.

    a. Data privacy discussions in the clinic heavily track public discourse on data sharing and research.
    b. Patients generally altruistic with data access.
    c. Generally greater trust in hospitals than government. Concerned about government access.
    d. CTRL increases trust, promotes dialog.
    e. Consent fatigue is visible. Worried about bias since wealthier, better educated patients are more likely to use. Concerned about declining testing due to data concerns.
    f. Public education needs, opportunities to build in more literacy and education into workflow. Other languages need support, in general interpreter use is high for these patient groups. Could streamline CTRL enrolment, get more champion genetic counsellors to promote adoption.
    g. Generally low active use of CTRL, partially due to the nature of these studies. Sees patients that are either innately interested in tech or data or are not. Also depends on type of condition, could introduce bias.
    h. High level of implicit trust in CTRL because of Australian Genomics reputation. Data stewardship already done well.
    i. Patients question how CTRL preferences will be effectuated.
    j. Limited time, increased steps, and more complex consent process for clinicians are barriers.

5) A national Coordinator for a clinical genomics study which uses CTRL to help manage patient consent.

    a. Flyers and education materials for patients and genetic counsellors important.
    b. In current program, every site has had at least some CTRL use where offered.
    c. Genetic counsellors need to see immediate benefits to justify cost of using. In some cases, genetic counsellors may be limited and therefor will not participate: no computers in consult room, generally time-limited, lengthy enrolment process takes a lot of time, leads to consent fatigue.
    d. Access to iPads in clinic, for example, as pre-requisite for dynamic consent use.
    e. Need to address time limitations, standardization of processes.
    f. REDCap generally more used (i.e. for surveys). Possibility to add functionality to CTRL. Also make better use of 2-way communication. Opportunity for adaptation/implementation playbook to help clinics.
    g. Generally positive experiences, especially from studies that have heavy patient involvement.

6) The human research ethics committee, which ensures clinical research studies are held to high ethical standards and has a role in allowing the use of CTRL and other software.

    a. Concerned about equality/justice in health outcomes.
    b. Consent fatigue is a topic, but not that different from static consent. Major challenge. Also, how information is perceived by the participant versus what the clinician means.
    c. HREC limited in software expertise, relying on certificate or declaration of security. Security is a big focus. HREC generally good at keeping the public pulse, not great at technically evaluating software systems.
    d. Not just for CTRL, but all software: iterative updates could change things. How to handle this? How to define significant change in this context that would trigger re-evaluation?
    e. One solution: define in outset what would be considered non-significant, and evaluate that as part of the process.

7) Two CTRL product owners, who are responsible for the development and implementation of CTRL within Australian Genomics.

   a. Future plans for scaling, also need professionalization.
   b. Strong trust requirements around actually effectuating consent choices and communicating that.
   c. Concerned about longevity of systems, negative impacts of removing CTRL.
   d. One topic is role of patient versus ethical boards. Individual consent places large burden on patient.
   e. Scaling concerns are generally operational, not technical. System can handle far more traffic. On-prem installation generally liked, but makes scaling a chore.

8) Hospital administrators, who have broad responsibility for how hospitals manage patient data and are involved in clinical studies.

   a. Authentication, credentialing, and access to digital health services are important topics. Also harmonization and standardization between services.
   b. Concerned about documentation, safety and hazards, fragmentation of services.
   c. Health records are a lost opportunity regarding data sharing.
   d. Difference between what people think they want versus what they actually want. Regarding data sharing, there is a default to not share data, since this is usually current practice. Some stakeholders tend to focus on risks rather than benefits. Big lost opportunity.
   e. Dynamic consent is an opportunity to re-frame what consent is, patient-research relationship.
   f. Risks surrounding unanticipated use greater than data breach. Need data breach incident response plan for when, not if, that occurs. Generally not seen as fault of hospital.
   g. Consent needs to be computable and include provenance, traceability. Clinical safety issue.
   h. Opportunity for feedback from research projects: two-way communication.
   i. Concerned about equity of access. Also authentication and credentialing: users might have a shared device, for example. Always need a paper back-up.
   j. Generally deep mistrust of government, but higher trust in research and academia.
   k. Need features like roll-back, provenance logging. Common in software, less common for health records.

3.4 CTRL risks and opportunities

A team from DNV with backgrounds in quality management, genetic testing, cybersecurity and human factors combined the outcome of the document review described in 3.1.1 and the stakeholder interviews described in 3.3 for potential risks and hazards and noted these in a risk register clustered by theme.

3.4.1 Risk register

Table 3. Risk register detailing the risks and opportunities identified through document review and stakeholder interviews, and their source where relevant.

Theme	Risk/opportunity	Source
Adoption	Challenges in collaboration with software developers and IT staff.	
Adoption	Cost of IT technical support.	
Adoption	Collaboration between involved parties.	

Adoption	Modification of database structure may cause issues downstream.	
Adoption	Databases have to be deployed in a secure environment, no integrated security.	
Adoption	Several research groups in Australia have shown interest in adapting the platform to their projects.	
Data breach	How to ensure all partners conform to data processing and data breach policy? How to check? How to enforce?	Data Management Plan 2019 Full_approved
Effectuating preferences	Do researchers have a responsibility to provide… "the opportunity for each participant to re-consider their decision related to receiving results or findings" as identified in National Statement on Ethical Conduct on Human Research (2018)?	GHFM Project plan proposal (grant application)
Effectuating preferences	Manual export preferences from CTRL to REDCap. If DB structure on either end changes or if data is corrupted, may not be clear to user.	Australian Genomics Architecture
Effectuating preferences	How does CTRL effectuate data sharing from the Australian Genomics Flagship Data? How (often) are patient preferences (in CSV) updated?	CTRL REDCap Metabase procedures
Effectuating preferences	Are culturally and linguistically diverse communities and research participants with low literacy sufficiently addressed?	GHFM Project plan proposal (grant application)
Effectuating preferences	Pilot study to assess use of CTRL: Participant unable to delete their own CTRL registration.	CTRL_Protocol_V2_clean
Effectuating preferences	Different interpretations of DUO codes in different organizations may lead to unanticipated data use.	DUO
Effectuating preferences	Use of DUO and text displayed may mismatch, leading to unanticipated data sharing (i.e. DUO:0000018 Not for profit and research institutions, which may have tech transfer offices).	DUO
Effectuating preferences	Explanatory text for DUO codes may be unclear to participants, leading them to input inaccurate consent preferences and the unanticipated sharing of data.	DUO
Effectuating preferences	There may not be DUO codes that reflect data sharing preferences of participant (i.e. opt-in to data sharing for clinical purposes, but not research).	DUO

Future implementations	How is CTRL packaged? Easy for other institutes to implement? Risk that implementation at other institutes introduces unforeseen issues.	
Future implementations	Coupling of CTRL and REDCap may lead to design choices that make future use difficult (i.e. when integrated with other study databases or LIS/LIMS)	Sano Genetics and Working Group Folders
Legal	Can minors withdraw/reconsent when they come of age? How does this workflow work?	
Legal	Insurance topics: need to disclose participation in genetic studies or testing.	CTRL screenshots_V1_24.9.19
Legal	Possibility for lost-in-translation in preferences between REDcap and CTRL (i.e. Consent to X interpreted or enforced slightly differently).	Metabase REDCap mapping
Liability and Ownership	Liability not very clear: Curve not liable, Australian Genomics is in MCRI, who acts as agent for other research institutions, therefor MCRI liable? Do they have enough insight into actions of other institutions? Points of contact: IT and HREC. Lack of accountability, unclear ownership.	Curve, CTRL website TACOS
Operational	Ruby on Rails as a niche language may make updating CTRL web app challenging due to limited developer availability. Other challenges?	
Operational	CTRL SQL DB therefor SQL injection possible?	
Operational	How much redundancy is there in CTRL & REDCap installations in MCRI?	
Operational	Changes to REDCap API or Data structure may mean CTRL does not receive response. May not be apparent to users.	Australian Genomics Architecture
Operational	Feedback to Curve - Australian Genomics must thoroughly test functionality, content and logic in two weeks.	Australian Genomics Administrator Portal - Proposal by Curve Tomorrow v1.1[1]
Operational	Curve reserves the right to change any warranty or service policy set forth in any product license or elsewhere, at any time, in a form of a written notification.	Australian Genomics Administrator Portal - Proposal by Curve Tomorrow v1.1[1]
Operational	Data shared stored, or accessible from - REDCap Study Database, CSIRO FHIR Server, Genomic data repository, Variant atlas, Gen-Phen Interface, Shariant platform - how do these communicate - more	Data Management Plan 2019 Full_approved

	info about these are in this document. Review when information is available - are there any resulting risks?	
Operational	Cloud IT service - role of Alfred Health cloud in data collation not entirely clear.	_200601_Cloud_IT_Service_Evaluation_Checklist_system_v1.6
Privacy	User may have Google token on PC when accessing CTRL (viewing YouTube video), user tracking by Google possible.	
Privacy	Significant personal data and health data held in CTRL: strictly necessary from data minimization perspective.	Australian Genomics DB Schema
Privacy	Personal data of non-users held in CTRL (ie. contact information for family members)	Australian Genomics DB Schema
Privacy	Participants' expectations may not match data collection/sharing activities indicated in TACOS and Privacy Policy (i.e. scope of data collected, scope of sharing with respect to partners or locations).	Privacy Policy
Privacy	In the event of a data breach, for any data created, managed and shared by Australian Genomics, data recipients will be required to notify security@australiangenomics.org.au immediately - have the processes following this been tested?	Data Management Plan 2019 Full_approved
Privacy	Is data transfer done according to GDPR? regarding encryption and other requirements?	
Privacy	How to ensure other parties are GDPR complaint re storage, processing, further transfer, and erasure?	
Privacy	Unclear language surrounding consent preferences in REDcap.	Metabase REDCap mapping
Privacy	Medical records from past 14 years may be collected for studies. There is an obligation to delete, but no timeline. Risk that management practice does not reflect participants expectations.	CTRL screenshots_V1_24.9.19
Privacy	We will collect information about you from the following databases through third party data linkage agencies: Who are these?	HIDDEN MMICF V2 2016.224 Marked up
Public engagement	Use of CTRL leads to less diverse populations due to lack of technology access.	HREC Application
Public engagement	Reliance on DC may reduce human involvement in the consent process.	HREC Application

Public engagement	Individualised ethical approval may increase admin burden.	HREC Application
Public engagement	Participants may experience consent fatigue.	HREC Application
Public engagement	Risk that genetic counsellors do not use/refer patients to CTRL because of reasons (tech barriers, competitor, lose control of data).	
Public engagement	(Pilot study to assess use of CTRL) It is thought unlikely that participants would attempt to formally withdraw from the pilot study using the web/app; they would more likely simply stop using it. So they may not consent anymore, just lose interest and 'forget their consents'?	CTRL_Protocol_V2_clean
Public engagement	CTRL use at appointment - no study ID, need hardware, recruiter must have sufficient knowledge of CTRL, paper documentation must still be used in addition. When is it most strategic to introduce it? Current automated email invite to sign up generated by REDCap - engagement of recruiting genetic counsellor can make or break inclusion.	Cardiac CTRL workshop 6th Feb
Security	The report with changes made during the day is emailed daily to australian.genomics@mcri.edu.au (v2-spoof possible? Data minimization: Why do you need this report at all? What does it do?).	CTRL v2
Security	Security assessment performed is for MCRI infrastructure and not for CTRL specifically.	
Security	CTRL passwords: 2FA? Probably hashed (from CTRL DB Schema field titles). Salt? Separate from MCRI passwords for Admin? Password reset poisoning possible?	Australian Genomics DB Schema
Security	MCRI has processes for PAC and is secure. Are there weaknesses that could impact CTRL?	Data Management Plan 2019 Full_approved
Security	MCRI has backups (nightly). Is this sufficient for CTRL?	Data Management Plan 2019 Full_approved
Security	MCRI performs 3rd party penetration testing 2x/year. Are there any CTRL-specific weaknesses that would be out-of-scope?	Data Management Plan 2019 Full_approved
Security	Browser/OS that is used may be outdated and have vulnerabilities. How to ensure that no users have browser/OS vulnerabilities?	

Security	Should be requirements for password set. Not only frequency of updates but password length, symbols, and other requirements.	
Security	HTTPS/TLS. Is this used?	
Security	How to make sure users never log on to the site using a public/otherwise untrustworthy network? Man-in-the-middle attacks possible?	
Security	Cross Site Request Forgery (CSRF). Can other websites interact with application in a malicious way?	
Security	Penetration testing done at MCRI. Who? What is done with results? CTRL specifically included in this?	
Security	Updating CTRL (by Curve) may introduce new security risks.	
Security	Frequency of app update: fast enough to close known exploits?	
Security	What test protocols are set up to catch any changes to CTRL? Or vice versa changes to REDCap?	

3.4.2 Failure Modes

Through review of the risk register, stakeholder interviews, and the entity map and CTRL workflows, three primary failure modes were identified (see Fig. 6) and subsequently presented to Australian Genomics in a collaborative workshop. The failure modes can be described as a limited set of 3 key conditions which can be caused by numerous types of upstream events from various risk categories, but that result in a set of concrete and predictable negative consequences for the various stakeholders which CTRL impacts. The three failure modes, data breach, data mishandling, and unanticipated consequences are described in more detail below.

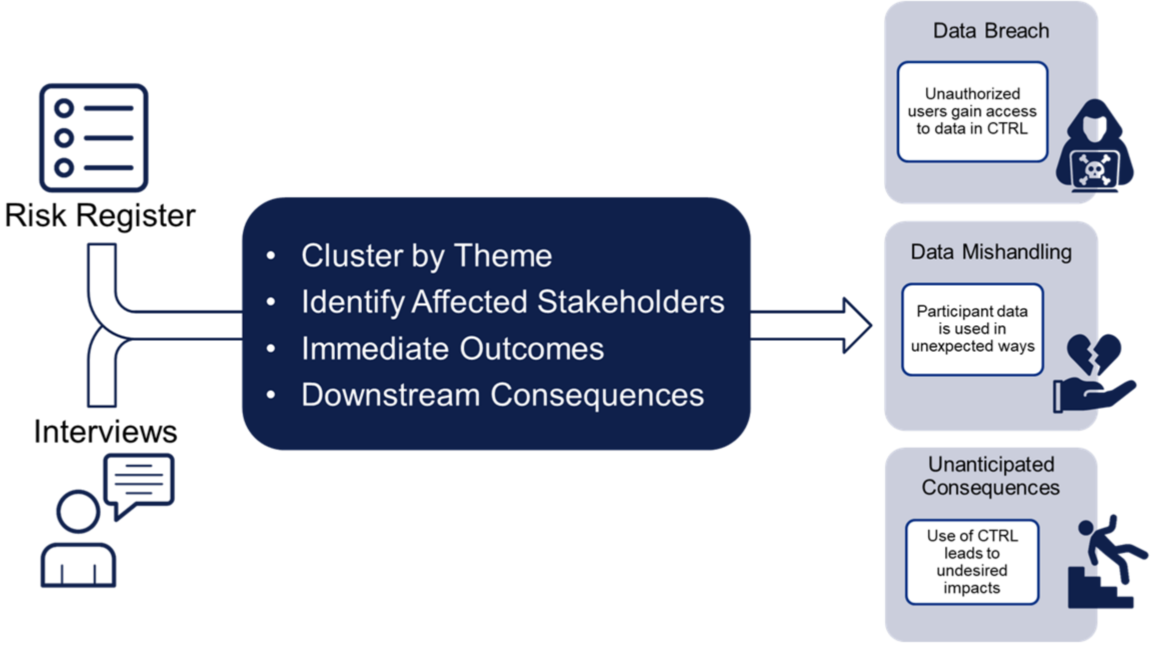

Risk Register
Interviews
Cluster by Theme
Identify Affected Stakeholders
Immediate Outcomes
Downstream Consequences
Data Breach
Unauthorized users gain access to data in CTRL
Data Mishandling
Participant data is used in unexpected ways
Unanticipated Consequences
Use of CTRL leads to undesired impacts

Figure 6. Methodology for synthesizing findings from the risk register and stakeholder interviews to generate three major failure modes: data breach, data mishandling and unanticipated consequences.

3.4.3 Data Breach: Unauthorized parties gain access to data in CTRL

Through exploiting one or more security weaknesses, participant data is accessed by parties without proper authorization. The risks that lead to this failure mode can include security weaknesses in MCRI infrastructure, in CTRL itself, or in client devices. Other organizational factors that could lead to this failure mode arise from the complex, multi-stakeholder activities regarding security, which is the responsibility of the MCRI IT team, the Australian Genomics CTRL team, Curve Tomorrow, and the providers of the software, devices, and infrastructure the research participant uses to access CTRL. Regardless of the root cause of a data breach, there are several immediate consequences, primarily faced by the research participants themselves whose data is now irrevocably in the public sphere. These consequences in turn can lead to potential impacts to Australian Genomics, ranging from a loss of trust in the organization or the research ecosystem in general, through the breach of additional, more sensitive MCRI IT systems, to potential legal liability.

Half of stakeholders interviewed identified data breaches as a concern and identified negative consequences for both the research participant as well as the research ecosystem in general: chiefly that a major data breach would lead to a public loss of trust and decreased participation in research. Stakeholders stated that they generally accepted that security was handled well, but that they lacked the specific backgrounds needed for confidence in this statement.

3.4.4 Data mishandling: Participant data is used in unexpected ways

Various technical and governance risks lead to this failure mode, in which participant data is used in a way not compliant with their wishes. Examples of governance risks that could lead to a trust breach include differences between how Australian Genomics and partner institutions interpret data use agreements. The lack of a shared understanding between Australian Genomics and the research participant could also lead to trust breaches: a participant may believe that their data will be processed in a certain way or by certain actors, while in reality that is not the case. Various technical risks can also lead to trust breaches, such as de-sync between the participant’s browser and the CTRL server.

Governance risks can also lead to trust breaches, such as if two institutions interpret data use codes differently. The combination of complex data sharing ecosystems both within and between organizations and the inability to effectively retract data once access has been granted were identified as key factors.

Most (8 of 9) stakeholders interviewed raised ethics and trust topics as key priorities. The chief concern was situations where participant data is used in a way with which participants would not normally agree. Multiple stakeholders stated that while general trust in the government is low, there is an overall high level of trust in the healthcare and research ecosystem in Australia, and that it is a top priority to maintain this.

3.4.5 Unanticipated Consequences: Use of CTRL leads to undesired impacts

In this failure mode, the use of CTRL leads to negative externalities on various stakeholders. The risks that lead to these unexpected consequences were more varied than in the other two failure modes, as were the specific outcomes. As an example, the use of CTRL could theoretically exacerbate health inequality: poorer, less educated, and more rural individuals could have less access to both high quality healthcare and digital services. Another commonly raised example is consent fatigue, where participants tend to either automatically opt-in or opt-out due to the presentation of too much complexity or over time. Several operational risks could also lead to unanticipated consequences: a lack of funding for the continued operations of CTRL could reduce confidence in the research ecosystem for participants that were previously using CTRL to actively manage their consent preferences, for example.

Again, the majority (8 of 9) of stakeholders interviewed raised concerns about unanticipated or undesired consequences arising from the implementation of CTRL, chiefly the use of digital dynamic consent systems leading to an increase in health inequality. The second most common concern was consent fatigue and the effects of consent fatigue on clinical workflows and participation in research.

3.5 Decision gate 1

This project was designed to include a decision gate between Stage 1 and 2, to determine progress and value of ADA and whether or not to proceed to Stage 2 after the delivery of Stage 1. If so, which single failure mode for CTRL to move from Stage 1 to Stage 2 would also be decided, to demonstrate the ADA framework and to initiate the continuous improvement cycle of Stage 2. After reviewing the failure modes and risk profile generated in Stage 1, Australian Genomics decided to proceed with Stage 2, and prioritized data breach as the target for assurance case building in Stage 2. A second decision gate at the end of Stage 2 allows for the process to be repeated with the other failure modes identified, should resources allow and the outcome from the first provide value (see Section 4.4 below).

4 STAGE 2: DEVELOPMENT OF ASSURANCE CASE

4.1 Introduction to Stage 2

Stage 2 of the ADA framework builds on the profiling of the asset performed in Stage 1 to provide an **assurance case**. The term assurance can be defined as any activity that provides “grounds for justified confidence that a claim has been or will be achieved" (ISO/IEC/IEEE 15026 – Systems and software assurance). These **claims** can be about any quality that stakeholders value, for example safety, sustainability, effectiveness or efficiency, and can be substantiated by providing and assessing **evidence** that supports these claims. Accordingly, assurance providers have an oversight function and provide justified confidence in the claims made about a system, both protecting and creating value.

Stage 2 of the ADA framework consists of the following steps summarized in Fig. 7 below: first, creating a strategy for generating an assurance case through formulation of a series of **claims** about the asset or solution being assessed. This is done by structuring claims and then substantiating them by collecting, providing and assessing **evidence** for them. Collectively the claims, their supporting evidence and reasoning behind them form the **assurance case**. Section 4.2 below describes how this was performed specifically for CTRL.

.

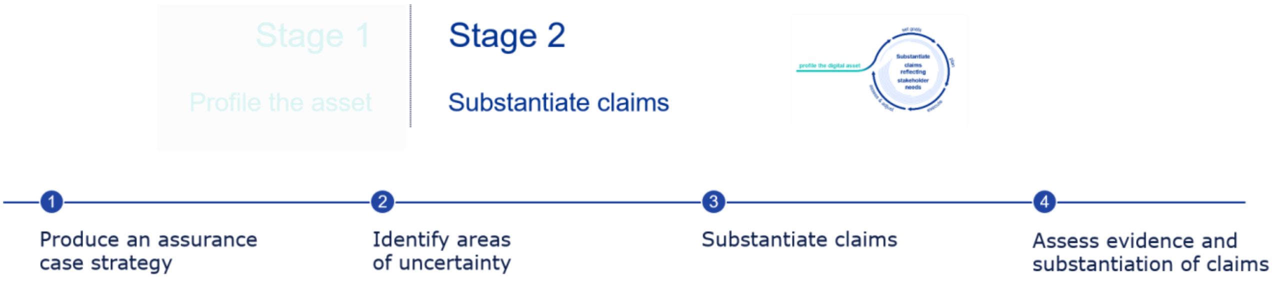
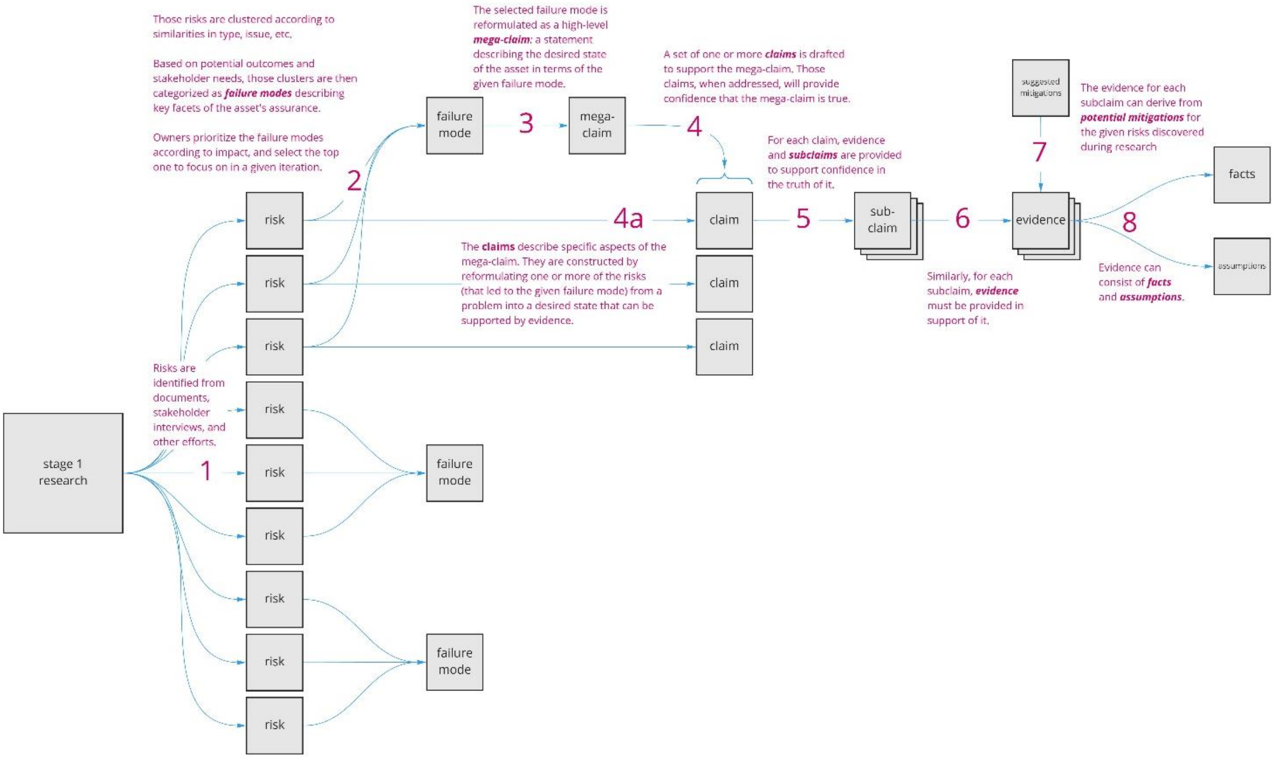

Stage 1
Profile the asset
Stage 2
Substantiate claims
profile the digital asset
set goals
plan
execute
assess & adjust
Substantiate claims reflecting stakeholder needs
1
Produce an assurance case strategy
2
Identify areas of uncertainty
3
Substantiate claims
4
Assess evidence and substantiation of claims

Figure 7. An overview of the activities performed in Stage 2 for building the assurance case.

4.2 Building of the assurance case for CTRL: Moving from failure mode to claims

This section describes the process employed to build an assurance case from the risks identified in Stage 1 for CTRL (see Fig. 8 below). In brief, a risk register was developed listing individual risks identified from document review, stakeholder interviews, the creation of an entity map and examination of data flows and use cases in CTRL (numbered Step 1 in Fig. 8). In Step 2, these risks were clustered according to theme and organized into three main failure modes describing the key facets of assuring CTRL. For initiating Stage 2, via a workshop-facilitated discussion, the owners of CTRL prioritized the failure mode related to data breach (Step 2), which was then reformulated into a top level claim (Step 3), in turn detailed by a set of sub-claims (Step 4). This set of sub-claims detail individual aspects of the main claim, which when sufficiently addressed, provides assurance and confidence that this claim is true. This is done by examining each claim (Step 5) and sub-claim (Step 6) in turn and providing evidence in its support, which can derive from potential mitigating actions associated with the risks identified (Step 7) and can consist of both facts and assumptions (Step 8).



Those risks are clustered according to similarities in type, issue, etc.

Based on potential outcomes and stakeholder needs, those clusters are then categorized as ***failure modes*** describing key facets of the asset's assurance.

Owners prioritize the failure modes according to impact, and select the top one to focus on in a given iteration.

The selected failure mode is reformulated as a high-level ***mega-claim***: a statement describing the desired state of the asset in terms of the given failure mode.

A set of one or more ***claims*** is drafted to support the mega-claim. Those claims, when addressed, will provide confidence that the mega-claim is true.

For each claim, evidence and ***subclaims*** are provided to support confidence in the truth of it.

The evidence for each subclaim can derive from ***potential mitigations*** for the given risks discovered during research

The **claims** describe specific aspects of the mega-claim. They are constructed by reformulating one or more of the risks (that led to the given failure mode) from a problem into a desired state that can be supported by evidence.

Similarly, for each subclaim, ***evidence*** must be provided in support of it.

Evidence can consist of ***facts*** and ***assumptions***.

Risks are identified from documents, stakeholder interviews, and other efforts.

Figure 8. Process for moving from risks and failure modes generated in Stage 1 to building the assurance case in Stage 2, by generating main and sub-claims that are substantiated by evidence that is provided.

4.3 Strategy for substantiating evidence and evaluating claims

This section details the evidence provided for the prioritized top level claim, that this implementation of CTRL provides sufficient data protection safeguards to justify its use in managing consent in this context, as well as its sub-claims.

Evidence provided to support the claims was obtained from pre-existing documentation relating to CTRL, including: user authentication and ethics protocols, architecture map, standard operating procedures, data management policies and MCRI IT privacy and security documentation. Evidence substantiated the claims made against the failure mode selected for in depth review, whilst also identifying areas where further investigation and testing would be required to ensure sufficient operational and technical measures are in place to protect user data.

Greater confidence in the process of evidence gathering could be gained by involving personnel peripheral to the project. For example, consultation with the software developer or MCRI may have resulted in additional or alternative evidence, given that CTRL project leads are not experts in all areas where evidence was required to support claims. Having access to examples of sufficient evidence or safeguards that would be required to substantiate claims would be beneficial to the process and stimulate thinking about areas for improvement. Opportunities were identified where future developments to CTRL or new projects could undertake a more extensive examination of the security measures currently in place and identify ways in which they could be strengthened.

The report will serve as a summary of evidence of the considerations in the development and use of CTRL, but importantly will also facilitate future strategic developments of CTRL and related products. Immediate next steps will include the CTRL team developing evidence for the claims related to the other two failure modes not selected for detailed examination as part of this project.

Table 4. Claims, sub-claims and evidence supporting the sub-claims

Claim	Sub-claim	Evidence
CTRL has sufficiently robust user authentication protocols in place.	Processes in place to verify user identity at account creation are sufficiently difficult to exploit.	• User verification by genetic counsellor: verify identity face-to-face and obtain email address from participant. • Risks: Couples sharing e-mail addresses, access to partners e-mail address. • Weakness not in the person identity confirmation, but rather participants personal management of email. • Australian Genomics checking between CTRL and REDCap for User verification issues (i.e. email does not match name of participant).
	User authentication processes are sufficiently capable of ensuring only the intended individual can be authenticated.	• Authenticated face-to-face, but CTRL email sent later. Even if a user is verified by genetic counsellor, a separate controller of email account can set password and will manage that CTRL account for all future interactions.
	Sufficient technical measures are in place to prevent insecure password management activities.	• A timed log-out is set up for CTRL so the user is automatically logged out after period of 10 min of inactivity. • Password is encrypted.
Sufficient safeguards are in place to ensure data received by the CTRL server is only provided by authorized users.	Sufficient measures are in place to ensure a secure, encrypted connection between an authenticated user and the CTRL server.	• Registration details for CTRL are only emailed to user once they have had a face-to-face appointment with the genetic counsellor, determining identity of user and their email address. • CTRL is hosted on secure institutional servers.
Sufficient safeguards are in place to ensure user workflows cannot be exploited to gain access to user data.	The initial user enrolment workflow cannot be exploited by common means.	• Initial enrolments into the Australian Genomics cardiac flagship are completed by genetic counsellor during face-to-face appointment and therefore cannot be exploited by common or external means. Future implementations of CTRL may be more vulnerable.
	The user login workflow cannot be exploited by common means.	• Specific unique user study ID given to each participant to register for CTRL so each registration has a unique pathway • CTRL portal not advertised or commonly known about online except the links sent to prospective participants, unlikely that someone not part of a study would attempt to enrol in the platform.
	The password reset workflow cannot be exploited by common means.	• Password reset linked to email address on original CTRL registration. Requested password reset would be sent to that email address. Participant responsibility to ensure no one else has access to email address.
Breach of other tools on the server will not lead to breach of CTRL.	Sufficient measures are in place to prevent access to data in CTRL in the event that other MCRI software is breached.	• Evidence is available in MCRI security protocols.
The infrastructure CTRL is installed on is	Physical access control measures at MCRI are sufficient to prevent	• Evidence is available in MCRI security protocols.

sufficiently resistant to common attacks.	unauthorized users from gaining access to MCRI infrastructure.	• Access to MCRI database for employees requires DUO and/or Otka authentication and specific usernames. • Access to specific programs/accounts on the MCRI database require employees to request access and for access to be specifically approved.
Sufficient measures are in place to monitor security.	Features are in place to log actions and activities in CTRL.	• Daily logs of changes to any account are emailed to CTRL team. • Daily logs set up to gather critical changes. In Metabase, can query anything. • Metabase (hosted in MCRI) is used to query CTRL database. • REDCap also logs activities (might have forensic value, not as an alarm). Can be used to investigate data integrity.
	Action logs in CTRL are generated and stored in a way that unauthorized users cannot access, modify, or delete them.	• Metabase: Read-out from CTRL database. • Email daily reports are in Excel, REDCap most fields can be edited. • Email logs are sent to multiple emails. Logs for day before are sent out at 07:00.
	Processes in place to identify and respond to security breaches are sufficient to limit the impact of security breaches on CTRL users.	• MCRI monitors suspicious activity. • Australian Genomics data breach response policy/SOP.

5 DISCUSSION AND CONCLUSION

The adoption and implementation of new technologies in the healthcare sector often consist of reconciling and integrating needs and requirements for multiple layers of architecture, user types, organizational, regulatory and legal regimens. The joint project was initiated and carried out with the aim of testing the suitability of DNV’s Assurance of Digital Assets (ADA) framework for providing assurance on the dynamic consent solution CTRL from Australian Genomics.

In Stage 1 of the framework, risks related to CTRL were gathered through documentation review, stakeholder interviews and examination of use cases and data flows, and structured into failure modes. In Stage 2, a prioritized failure mode was reformulated into a claim and its subclaims, before gathering evidence to substantiate these claims, thus initiating the iterative process and continuous improvement cycle of building and maintaining an assurance case.

The results demonstrated utility in applying and providing a systems perspective on a healthcare technology, providing the owners a fuller overview of the system and where and how risk reduction actions could be taken and monitored. This allowed the examination of CTRL’s three layers of stakeholders, namely participants in healthcare research (and the public), individual research organizations and inter-organizational research, and by building of the assurance case and substantiating claims, facilitating the closing of the trust gap between these three layers for the successful implementation of CTRL. Ultimately, applying ADA framework to CTRL supports a systems approach for identifying and closing substantial trust gaps that may further support the successful implementation and scaling of CTRL.

This project is subject to several limitations and therefore results should be interpreted with caution. This is the first application of the ADA framework to a healthcare use case, with the ADA methodology still under development. Additionally, a deeper examination of the relevant legal and regulatory requirements governing the implementation of CTRL, potentially including individuals with legal expertise, was out of scope for the purposes of this project, but may be considered as this may shed some additional light on the risk and opportunity landscape for CTRL.

An additional outcome of this project was the opportunity it allowed for further development and improvement of the ADA framework. Templates and work guides for different steps in Stages 1 and 2 were developed and matured that are suitable for other use cases. Specifically, Stage 2 of the methodology would benefit from further implementations and refinements to allow for smooth transferability to the owner for continued monitoring. Finally, the ADA framework was initially designed for generic application across industries, but learnings from using ADA on a healthcare use case demonstrates its value and utility in this sector.

6 ACKNOWLEDGEMENTS

The authors would like to thank the numerous stakeholders interviewed during this project, whose perspectives, insights, and collective experience serve as the foundation of this work.

7 GLOSSARY OF TERMS AND REFERENCES

7.1 Glossary of terms

ADA: DNV's Assurance of Digital Assets framework

Assurance: The results of any activity that provide grounds for justified confidence that a product or process is fit for purpose and that it complies with existing safety, environmental, societal, or regulatory requirements. The provision of assurance is always based on credible and relevant evidence.

Assurance Case: A structured set of arguments and a body of evidence that shows how an information system satisfies specific claims with respect to a given quality attribute.

Claim: An assertion that something is true. Claims can be supported by evidence, objective or subjective judgements, or subordinate claims as part of an assurance case.

CTRL: Inspired by dynamic consent, CTRL is a web-based application developed by Australian Genomics that has been designed to increase participant choice and autonomy in decision making and opportunities for ongoing participant engagement.

Failure Mode: A failure mode describes the potential ways in which a system could fail to achieve one of its intended functions. There can be multiple, unrelated causes or precipitating events that can lead to a failure mode, and there can be multiple downstream effects on other systems or stakeholders. Mitigating actions or systems can be put into place both to reduce the probability of failure as well as to reduce the severity of a failure.

GDPR: The General Data Protection Regulation (EU) 2016/679 is an EU law regulating data protection and privacy.

HREC: (Human Research Ethics Committee) A committee which ensures clinical research studies are held to high ethical standards and has a role in allowing the use of CTRL and other software in research projects. Equivalent to Research Ethics Committees and Institutional Review Boards in other countries.

Metabase: A business intelligence tool.

REDCap: (Research Electronic Data Capture) is a commonly used secure, web-based application for data capture in research studies.

Risk: The potential for a negative event to occur, encompassing both the probability of occurrence of harm, and the severity of that harm.

Top level claim: A statement describing the desired state of the asset in terms of the given failure mode.

7.2 Citation

DNV. (2022, March 2022). Assurance of Digital Assets (ADA) assessment of CTRL: a collaborative project of Australian Genomics and DNV. Retrieved from https://www.dnv.com/research/healthcare-programme/

7.3 References

/1/ Assurance in the Digital Age: The ADA Framework. DNV internal white paper (2021). Available on request.

/2/ 'CTRL': an online, Dynamic Consent and participant engagement platform working towards solving the complexities of consent in genomic research. Haas MA, Teare H, Prictor M, Cegregra G, Vidgen ME, Bunker D, Kaye J and Boughtwood T *Eur J Hum Genet* **29,** 687–698 (2021). https://doi.org/10.1038/s41431-020-00782-w

/3/ Research electronic data capture (REDCap) - a metadata-driven methodology and workflow process for providing translational research informatics support. Harris PA, Taylor R, Thielke R, Payne J, Gonzalez N and Conde JG. *J Biomed Inform* **42**:377-81 (2009). https://doi.org/10.1016/j.jbi.2008.08.010

DNV

About DNV

DNV is the independent expert in risk management and assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions.

Whether assessing a new ship design, optimizing the performance of a wind farm, analyzing sensor data from a gas pipeline or certifying a food company’s supply chain, DNV enables its customers and their stakeholders to make critical decisions with confidence.

Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world’s most successful and forward-thinking companies.