The Impact of General Data Protection Regulation on the Australasian Type-1 Diabetes Platform

Zhe Wang, Anthony Stell, Richard O. Sinnott and ADDN Study Group*
School of Computing and Information Systems, The University of Melbourne
Melbourne, VIC 3010, Australia
Emails: {zoe.wang1,anthony.stell,rsinnott}@unimelb.edu.au

2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS) | 978-1-6654-6770-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/CBMS55023.2022.00043

***Abstract*—Australia is a region with a high incidence of diabetes with approximately 1.2 million Australians diagnosed with this condition. In 2012, the Juvenile Diabetes Research Foundation (JDRF – www.jdrf.org.au) provided funding to establish the national registry - the Australasian Diabetes Data Network (ADDN – www.addn.org.au) populated with extensive longitudinal data on patients with Type-1 Diabetes (T1D). The ADDN registry has evolved over time and now includes data on over 20,000 patients from 22 paediatric centres and 11 adult centres across Australasia, i.e., where the data is uploaded from hospitals and not manually entered. This data has historically been de-identified at source, however moving forward there is increased demand from the clinical research community to link between data-sets using fully identifying data. In this context, this paper explores the challenges this poses with regards to the evolving processes that must be incorporated for data collection and use, e.g. e-Consent, and especially the impact of General Data Protection Regulation (GDPR) on the ADDN processes.**

***Keywords*—ADDN, GDPR, Type-1 Diabetes, Privacy, Consent.**

I. Introduction

Approximately 130,000 Australians have been diagnosed with type-1 diabetes (T1D), Australia has the seventh-highest prevalence of T1D in children aged 0-14 in the world and sixth highest more general incidence rate [1]. The Australasian Diabetes Data Network (ADDN – www.addn.org.au) was established to provide a national registry to collate T1D data from initially paediatric centres and subsequently from adult centres across Australia and New Zealand. At present, the registry includes longitudinal data on over 20,000 patients with over 230,000 visits/treatments from 22 paediatric diabetes centres and 11 adult diabetes from across Australia and New Zealand. The major objectives of ADDN are to provide opportunities for monitoring long-term clinical outcomes, to facilitate research studies and to improve clinical care. The legal and administrative context of a project like ADDN continues to evolve however with initiatives such as General Data Protection Regulation (GDPR) and their national equivalents (such as the NZ Privacy Act 2020) becoming increasingly important globally. Furthermore, researcher demands and expectations on ADDN data and the ability to link with both internal (tracking patients across sites, e.g., from paediatric to adult centres) as well as with external data resources increasingly depend on use of identifying data. This paper explores these issues and what they mean for ADDN moving forwards.

*The ADDN Study Group: https://www.addn.org.au/governance

A. ADDN Implementation

The software and database support and maintenance of ADDN are provided by Melbourne eResearch Group (MeG – www.eresearch.unimelb.edu.au) at the University of Melbourne. Clapin et al. [2] describes the initial phase of development up to 2016 where the focus was primarily paediatric data coordinated with the the Australasian Paediatric Endocrine Group (APEG[1]). Through coordination with the Australian Diabetes Society (ADS[2]) the platform has since evolved to include many adult sites both in Australia and New Zealand. The platform is realised as a mature web application utilizing the Java-based Spring framework, which supports a Model-View-Controller (MVC) paradigm and provides a RESTful Web Service interface, connecting to a PostgreSQL database. The view layer (frontend) is served by a Thymleaf template engine.

As shown in figure 1, the Data Cleaning module defines the data processing pipelines including the logic of Extraction, Transformation, and Loading (ETL) functionalities. Participating centers have historically uploaded de-identified patient data from their local databases through the ADDN dashboard every 6 months. A major challenge here has been the heterogeneity of datasets extracted from hospital/center-based clinical systems. A unified data dictionary (agreed with APEG/ADS) containing 141 data points was developed based on national health data standards [3] where available. Data points are related to five fields: patient fields (demographic characteristics, consent information, etc.), co-morbidity fields, family history fields, visit fields (clinical measurements, therapeutic interventions, etc.), and medication fields. Certain rules such as data type, lower and upper bound are specified. A canonical XML data schema implementing the data dictionary is used for data validation and generating error reports to ensure continuous data quality and integrity -Fig. 2 shows an example of the current schema. With the latest release, the dashboard also supports automatic schema upgrading, Excel data conversion and error correction. Universal Subject Identifiers (USI) generated from the BioGrid data linkage platform[3] are used by centres to create unique identifiers for

[1]https://apeg.org.au/
[2]https://diabetessociety.com.au/
[3]https://www.biogrid.org.au/

2372-9198/22/$31.00 ©2022 IEEE
DOI 10.1109/CBMS55023.2022.00043

patients. These are then merged with the patient data and uploaded to the PostgreSQL database.

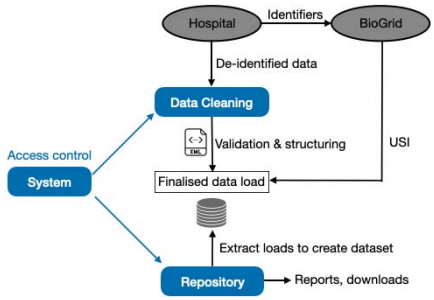

Fig. 1. Architecture of the ADDN registry and Data Pipelines

```
<patient>
  <centre>NSW_NTL_JHC</centre>
  <primaryCentre>true</primaryCentre>
  <localId>12345</localId>
  <dateOfAddnConsent>2022-01-01</dateOfAddnConsent>
  <consentToBeContacted>true</consentToBeContacted>
  <countryOfBirth>1102</countryOfBirth>
  <diabetesType>TYPE_1</diabetesType>
  <dateOfDiagnosis>2014-01-01</dateOfDiagnosis>
  <countryAtDiagnosis>1101</countryAtDiagnosis>
  <dkaAtDiagnosis>false</dkaAtDiagnosis>
  <phLevelAtDiagnosis>7.5</phLevelAtDiagnosis>
  <bicarbonateLevelAtDiagnosis>23</bicarbonateLevelAtDiagnosis>
  <bioGridId>1234</bioGridId>
</patient>
```

Fig. 2. A representative example of de-identified data based on the current schema

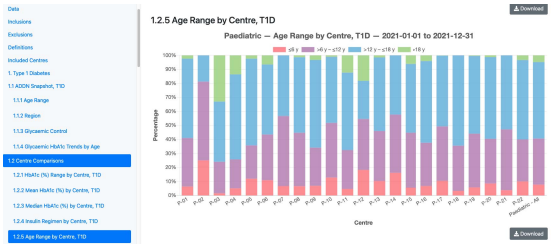

Fig. 3. Benchmarking reports

The registry provides a user interface for hospital-based ADDN research teams to create final (clean) datasets collated from their (local) data loads. This process may include multiple upload steps where the centres have to address warnings, e.g. data outside of expected ranges or data missing completely. Once cleaned, validated and uploaded, different types of reports can be generated including online and interactive benchmarking reports for each centre (Fig. 3). Completeness reports are used to provide feedback to each centre on their overall data quality.

The system also allows registry administrators to grant security levels to users. All users require usernames and passwords to log in. Different permissions exist including system administrator, repository administrator/viewer, data cleaning administrator/viewer, load creator/reviewer, etc. These are assigned to each individual user. The ADDN data access model is described in [2].

All of the data sent to ADDN is SSL-encrypted (256-bit SSL-encryption). The data is stored securely and indefinitely on a server owned and managed by The University of Melbourne in a physically secure data centre.

B. Ethics and Security of ADDN

The privacy legislation in the different states of Australia and New Zealand vary. Historically opt-out consent was the basis for ethics and data sharing across ADDN since the data was de-identified at source before being uploaded to ADDN. Even with this however, institutional research governance approval was required for each participating centre.

As mentioned, currently ADDN has collected de-identified data, i.e., where the identifying information of patients is not included in the registry uploads from hospitals. Rather unique subject identifiers (USI) are generated using the BioGrid data linkage platform and incorporated into the data uploads (shown in Fig. 2 as the ”bioGridId”). The USI is generated by a small set of participant identifiers including name, parts of medicare number, date of birth and gender provided by hospitals. This allows data linkage across datasets or within the same dataset, for example, to track a patient from paediatric centre to adult centre by merging data using the unique ID. The accuracy and robustness of the BioGrid USI scheme has proven to be limited within ADDN. Furthermore, moving forward the clinical research community wish to link T1D patient data with a range of official external resources such as the Pharmaceutical Benefits Scheme (www.pbs.gov.au), the Medical Benefits Scheme (www.mbsonline.gov.au) and the National Death Index from organisations such as the Australian Institute of Health and Welfare (https://www.aihw.gov.au). Without significant structural re-engineering, this necessitates that fully identifying data is included in the registry. This raises both technical, legal and ethical issues on data collection and usage. Many of these issues become more obvious when viewed in the context of legislation such as the General Data Protection Regulation (GDPR) [4].

II. GENERAL DATA PROTECTION REGULATION

Hitherto, the ADDN platform has been developed within the context of Australian legislation such as the Privacy Act 1988 (The Act) [5]. However this legislation is under review to bring it in line with international frameworks such as GDPR [4, 6, 7]. It is widely recognised that medical research across Australasia needs to consider the protection of participants' data from a global perspective. Compared to the current Privacy Act, GDPR enumerates the scope of personal data and sets the legal basis upon which access, use and sharing of sensitive health data can be achieved. At the core of the GDPR is the idea of empowering an individual (or ”data subject”) by allowing them to know about what data is being collected on them, where it is located and how it is subsequently accessed and used. GDPR introduces a range of concepts to deal with these issues.

A. GDPR Controller, Processor and Data Subjects

The GDPR defines the concepts of *data controller* and *data processor* (Article 4.7, 4.8). These are subject to different obli-

gations. According to the GDPR, the controller is the "entity that determines the 'why' and the 'how' of processing personal data" whilst the processor is "the entity that actually performs the data processing on the controller's behalf". In ADDN, in common with many multi-party collaborations, there is a complex chain of parties that perform duties related to both the data controller and data processor concepts. The main director of operations of ADDN are the ADDN data governance team comprised of independent (external) researchers, ADDN investigators, representatives from JDRF and patient advisory group representatives. The data of subjects comes from participant hospital systems into this governance structure, which through various layers of management and operation, filters through to processing by the software and infrastructure developers at the Melbourne eResearch Group (MeG).

GDPR also defines the concept of a *data subject* as "any living individual whose personal data is collected, held or processed by a particular organisation."(Article 4.1). Patients that participate in ADDN are data subjects and hence any personal data related to the data subjects needs to be protected by the regulation. The immediate question that falls from this definition is what is personal data.

B. Personal Data

GDPR regards personal data as "any information concerning an identified or identifiable natural person" (Article 4.1). This may be indirectly identifiable information hence GDPR identifies that all reasonable means that may be used to identify a person should be accounted for to determine if a person is potentially identifiable. Whilst the GDPR does not specify exact examples of Personally identifiable information(PII) (relying instead on precedent case law), the US Health Insurance Portability and Accountability Act (HIPAA), gives a summary of personally identifying information, which is instructive. It groups them into 18 identifiers including: name, address, including all geographic subdivisions smaller than state, such as street address, city county, and zip code; all elements (except years) of dates related to an individual including their birthdate, admission date, discharge date, date of death, and exact age if over 89; telephone numbers; fax number; email address; social security number; medical record number; health plan beneficiary number; account number; certificate or license number and vehicle identifiers and serial numbers, including license plate numbers.

To be considered "de-identified", in GDPR terms, a data controller must remove all such identifiers. One common method to achieve this is pseudonymisation, where identified information is replaced by a unique key code by hashing or other technologies [8]. According to GDPR, pseudonymisation is a safeguard of personal data but pseudonymised data is still personal data, if "it could be attributed to a natural person by the use of additional information"(Recital 26).

Moving forward, it has been proposed ADDN support the inclusion of a small set of participant identifiers including the patient name, date of birth and gender that would allow internal/external data linkage noting that T1D is a common condition and the chances of false positives exist compared, for example, to rarer diseases with fewer patients.

III. GDPR Legal Bases

According to GDPR [4], there are six legal bases (Textbox1) that organisations must choose from when processing personal data. If one of these legal bases is fulfilled, processing "special categories of personal data" in the context of medical research is still prohibited unless one of the specific legal bases in Textbox2 is satisfied.

A common legal basis in Textbox1 and Textbox2 is related to informed consent. In GDPR, the definition of "consent" is narrowed to "freely given, specific, informed and unambiguous, by a statement or by a clear affirmative action" (Article 4.11).

Textbox1 . The six legal bases for processing personal data (Article 6.1) [9]
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Textbox2. Specific legal bases to processing special categories of personal data in the context of medical research (summarised from Article 9.2) [9]
(1) Explicit consent is given by data subjects to process those personal data for one or more specified purposes... (9.2(a))
(2) Necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (9.2(c))
(3) necessary for reasons of public interest in the area of public health, such as ..., on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject. (9.2(i))
(4) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)... respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (9.2(j))
(5) Necessary for preventive or occupational medicine, medical diagnosis, provision of healthcare etc. based on member state or Union law and subject to professional secrecy (9.2.h and 9.3);

In the absence of (b) or (c), which would be trivial to establish, the medical research controller needs to work out whether they are pursuing a vital interest (d), where Recital 46 defines vital interest as "necessary to protect an interest which is essential for the life of the data subject or that of another natural person". Legitimate interest (f) is a more flexible basis - to determine if a legitimate interest is indeed legitimate, one should ask "can individuals reasonably expect their data to be used in that way?" and "do those legitimate interests

outweigh the privacy interests of the data subjects?" The "interest" here can refer to many things including some forms of commercial interests or societal benefits, for example, when the data subject is a client of the controller (Recital 47). The contour of public interest (e) is up to the EU and national law in GDPR (Article 6.3). In it's pursuit of GDPR equivalency, the Australian Law Reform Commission (ALRC) identify that public interest and privacy should be considered as a balancing exercise [10], where the Australian Government Department of Health [11] should be responsible for issuing public interest certificates to researchers under strict restrictions.

In the context of ADDN, there is no contractual service (b), legal obligation (c) or vital interest (d) that is applicable. However, public interest (e) and legitimate interest (f) may be considered in the context of Australian national law, where privacy and public interest needs to be counterbalanced. Thus, ADDN's mission of improving diabetes management and outcome could fall into the "public health and safety" category of public interest. However, this needs certification issued by the Department of Health and could not be the sole legal basis for processing of personal data. As such, informed consent (a) cannot be exempt for ADDN if it wishes to be GDPR compliant.

For a legal basis as described in Textbox2 to process sensitive health data, the data controller should consider if the process satisfies vital interest (2) as discussed above. Both (3) and (4) require that appropriate safeguards exist, e.g. pseudonymisation and encryption are two examples of technical safeguards that minimise data disclosure risks (Recital 156). In short, (3) demands public interest + safeguards whilst (4) focuses on scientific research purpose + safeguards. (5) is typically considered in the context of clinical trials. It is noted that "Research" is not actually defined in GDPR [9]. Recital 159 interprets scientific research in a broad manner, "including technological development and demonstration" and covering "fundamental research, applied research and privately funded research". It has also been debated whether commercial research should benefit from research exemption [9, 12].

For ADDN, (2) and (5) can be easily excluded. Pseudonymisation conducted for patients' data and the ethics committee responsible for governance are the safeguards of sensitive data processing. Under this premise, 'public interest' (3) might be considered as a legal basis, and it is also safe to say that scientific research (4) is one of the core bases for ADDN, i.e. aggregation of such large scale, longitudinal data is essential for many research endeavours.

Concluding this evaluation - to meet the criteria of at least one legal basis in both Textbox1 and Textbox2, without a valid public interest certificate in place, informed consent would be, in the end, a mandatory requirement for processing patient personal data in ADDN. The current default opt-out approach would not be sufficient to meet the explicit consent process required by GDPR legislation and its equivalents.

IV. GDPR and Consent

As discussed above, informed consent is the common legal basis to process personal data and sensitive information. It is also the legal basis ADDN will likely need to rely upon moving forward. Consent is only valid when it meets the conditions in Textbox3:

Textbox3. Conditions of Consent (Article 7 [4])
(1) **Freely given** - the data subjects must not be cornered into agreeing, noting that the imbalance between the data subject and controller can often making unencumbered consent difficult, e.g. patients may feel obliged or have concerns that the treatments they receive may be inferior if they do not agree. Furthermore, each usage of personal data should be given separate consent.
(2) **Specific** – the consent must be collected for certain agreed activities or purposes unless explicitly identified as "general" research.
(3) **Informed** - the data subject must fully understand the consent before making the decision including an understanding of data processing activities and their purpose and any associated risks or consequences.
(4) **Unambiguous** – it should be immediately clear whether the data subject has consented. Consent under GDPR cannot be implied, explicit opt-in consent is required.
(5) **Withdrawal** – individuals can withdraw their consent at any time, and this withdrawal should be made as easy as obtaining the original consent.

Furthermore, since the ADDN program integrates data from (at present) 22 paediatric centres across Australasia specific consideration should be made with regards to young adults/children. Consent from a child to process personal data shall be lawful where the child is at least 16 years of age under GDPR - noting that the Australian Paediatric Research Ethics and Governance Network (AGPREG) requires consent for individuals at least 18 years of age. Below this age, researchers need to get consent from both child and the parents or guardians [14].

In the above context, to collect data and conduct research with T1D patients data, the data controller and processor would need to leverage technology in an appropriate manner to ensure that opt-in consent is captured and is subsequently secure and auditable.

V. Background and Related Work

Mobile health (mHealth) is a term used to describe the use of mobile communication devices, such as mobile phones, tablets and wearable devices for health service delivery, data collection and medical research [15]. Usage of mHealth has been rapidly growing with the improvement of communication technologies. In Australia, 79.60% of the population owned a smartphone in 2022, which is the second-highest smartphone penetration rate in the world [16]. The popularisation of mobile phones have led to the development of mobile health applications having various functionalities [17, 18].

MHealth applications typically address temporal, geographical, and organizational barriers of clinical research and health service [19]. A patient, a doctor, a healthcare provider or a researcher can easily access the medical records anywhere and anytime using mobile devices. This can bring patients "into the loop" by enhancing patients' empowerment and autonomy. Several works have explored patients' active involvement with mobile applications. For example, Baysari et al. [20] examined

TABLE I
STAGE1: A GDPR-COMPLIANT MOBILE APP WITH ASSOCIATED SYSTEM CAPABILITIES

Capability	Details
Obtaining informed consent and generating associated (documented) PDF	Visual consent flows can be easily created with the ResearchKit consent module.
Optional informed consent comprehension test	Following the participant-centred consent approach by [13], a configurable survey style (ORKQuestionStep) module is used to confirm consent, in line with the "informed" condition of GDPR consent.
Consent withdrawal	Participants are able to withdraw their consent at any time (ORKConsentSectionTypePrivacy) to meet the "easy to withdraw" requirement in GDPR.
Specific real-time consent tasks	ADDN team can create consent tasks (ORKTaskViewController) anytime and deliver them through the app. Use cases includes dynamic consent forms related to researcher patient data access requests, requesting additional data from specific patients, or when patient data is to be transferred to another entity or linked with other external datasets.
Data privacy and security practices	The ResearchKit framework does not include a data management solution however the ADDN research team has the entire control of data storage, transfer and access.
View and visualise patients' data	With or without agreeing to participate in ADDN related research, users should be able to access all the functionalities provided by ADDN after logging in with regard to "their" data. This is important for the "Freely given" condition, where patients are not cornered into agreeing.

how "human factors" can facilitate patient-centred care coordination by enhancing the design of mHealth apps. Qudah et al. [21] thematically analysed the impact of mHealth applications on the relationship between patients and healthcare providers, where they found that mHealth apps can connect patient and healthcare providers to generate better health outcomes.

While most surveys focus on user experience and efficacy of mHealth apps, only a few of them focus on personal data protection. Schairer et al. [22] emphasised the role that electronic informed consent (e-consent) played in the age of mHealth to handle patients' personal data in a transparent manner, to mitigate the many unforeseen privacy risks that their data may be exposed to when existing in complex mHealth ecosystems.

The benefits of e-consent can only be realized with proper design. Nouwens et al. [23] revealed the "dark pattern" of e-consent, where the design tried to guide users into desired behaviour, for example, some websites try to increase the consent rate by deleting opt-out options. This behaviour violates the "withdraw" condition in Textbox3. Utz et al. [24] conducted various experiments on websites to investigate the impact of notice position, nudging, and offered choices on users' consenting behaviour, the results indicated the importance of graphic user interface design to free consent behaviour.

O'Connor et al. [25] explored the vision and voice of e-consent. They animated complicated GDPR and Terms & Conditions to help understanding. Wilbanks et al. [13] addressed two main challenges of e-consent, 1) the traditional method which doesn't emphasize the comprehension of users, and 2) users tend to skip over screen text when reading or even click "agree" without reading them. A participant-centred consent was proposed including a "pictorial" dominated first tier and a text dominated second tier, with a short assessment to make sure users understood the consent. The approach aimed to educate users about terms and conditions, benefits and risk, and has since been widely integrated into Apple's ResearchKit framework, supporting medical research projects such as Parkinson disease mobile data collecting [26].

A. ADDN Implementation Plans for e-Consent

It is noted that the vast majority of mHealth mobile apps have their own specific terms and conditions statements that individuals, such as T1D patients, agree to when signing up to use the app. However, this one-to-one connection between the app that the user installs, and the T1D patient, cannot be guaranteed within ADDN. Thus, centres will have thousands of patients and their data is collected as part of routine care in a given hospital setting. The "downstream" use of this data within ADDN currently happens without their full, explicit opt-in consent. It is also noted that many patients have deceased. Reconnecting the patient into the heart of the process is essential for ADDN to ensure it's GDPR compliance.

There are many technical approaches that have been applied for obtaining e-Consent, but these have largely been direct 1-1 forms of consent, e.g. consent to collect specific data from a specific patient using a given app. ADDN obtains and uses data captured as part of routine healthcare. Given this, it is essential that any solution works across all centres and healthcare settings and most importantly work for the patients themselves. This has multiple technical demands as discussed in I. Introduction.

The ResearchKit[4] is an open-source framework introduced by Apple in 2015, it helps mHealth research studies to streamline the process of screening and consenting patients. It provides a dedicated consent module to create customised informed e-consent, where users can interact with the visual consent step, review the detailed consent document, agree or disagree to consent, share consent to other controllers and withdraw consent. ResearchKit works seamlessly with CareKit[5], a framework that helps users follow care plans and share information with health care providers. This enables patients to log their symptoms and other health data and subsequently helps them track their health data. ResearchKit and CareKit have been successfully applied to many mHealth applications to facilitate medical research [26]–[28]. Whilst

[4]http://researchkit.org/

[5]https://www.researchandcare.org/

most of them have been applied in adult settings, [29] proposed and developed iCanCope app, which adopted ResearchKit for a paediatric research environment with high adoption rates. These proof-of-concept observation studies showed the potential of ResearchKit in building medical research apps for both adult and paediatric population.

The first stage of implementation of the ADDN app aims to offer a GDPR compliant app using the ResearchKit framework. Six core capabilities are required as shown in Table. I. This will support initial informed consent and associated comprehension assessment, consent withdrawal, and continuous consent assessments, e.g. if a researcher wishes to use the patient data in a linkage study, providing direct access to all of the patient related data captured by the ADDN registry and is a simplified way to visualise and understand their data.

Building on this, the app can also be used to collect further data that would complement the ADDN registry data, e.g. exercise or dietary data. The active task module of ResearchKit can also help to collect activity data such as motor activities, cognition, speech, and hand dexterity. As the implementation work on the ADDN app has just commenced, the next natural strategic step will be to adapt the application to use ResearchStack[6] for Android, in order to broaden the user-base across the eligible population as widely as possible.

VI. Conclusions

This paper has described the ADDN platform and the challenges it faces with regards to GDPR compliance as well as dealing with researcher demands for access and use of fully identifying patient data, e.g. for data linkage studies. The core challenge is moving from the current opt-out consent model to a fully informed patient opt-in consent model. This requires that patients are active protagonists within ADDN as opposed to the passive roles they currently play.

There are several challenges in the delivery of the ADDN app and the proposed capabilities it should offer. Targeted distribution is one: ADDN data is collected through routine healthcare processes and as such, the app would need to align in a functionally transparent way with routine healthcare environment settings. Other challenges include the heterogeneous, and often incompatible, nature of state health systems; the requirement of active advertising of the app by clinicians; and effective security operations authorizing valid patients versus random downloads from the respective app stores. However, the first steps outlined in this paper indicate an active and positive move towards ensuring explicit consent captured in a technological process that satisfies the high legal constraints required by the advance of digital legislation.

Acknowledgement This research was conducted as part of the Australasian Diabetes Data Network. We are grateful to JDRF Australia, the Australian Research Council and to the children and young people with diabetes and their families who provided the data. This research was supported by JDRF Australia, the recipient of the Australian Research Council Special Research Initiative in Type 1 Juvenile Diabetes.

[6]http://researchstack.org/

References

[1] "NDSS." https://www.ndss.com.au/about-the-ndss/diabetes-facts-and-figures/diabetes-data-snapshots/
[2] H. Clapin *et al.*, "Australasian diabetes data network: Building a collaborative resource," *Journal of Diabetes Science and Technology*, vol. 10, no. 5, pp. 1015–1026, 9 2016.
[3] "Metadata Online Registry (METeOR) website." https://meteor.aihw.gov.au/content/index.phtml/itemId/181162
[4] "EU G. General data protection regulation." https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] "Privacy Act 1988." https://www.legislation.gov.au/Details/C2014C00076
[6] Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues paper," 10 2020. https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/
[7] Attorney-General's Department, "Privacy Act Review – Discussion paper," 10 2021. https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/
[8] E. U. A. for Cybersecurity (ENISA), "Pseudonymisation Techniques and Best Practices—Recommendations on Shaping Technology According to Data Protection and Privacy Provisions," 2019.
[9] E. B. van Veen, "Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate," *European Journal of Cancer*, vol. 104, pp. 70–80, 11 2018.
[10] "ALRC." https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/8-balancing-privacy-with-other-interests/meaning-of-public-interest/
[11] "Public Interest Disclosures — Australian Government Department of Health." https://www.health.gov.au/about-us/corporate-reporting/public-interest-disclosures
[12] J. Meszaros *et al.*, "AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?" *Computer Law and Security Review*, vol. 41, 7 2021.
[13] J. Wilbanks, "Design issues in e-consent," *Journal of Law, Medicine and Ethics*, vol. 46, no. 1, pp. 110–118, 3 2018.
[14] rebeccalennon, "Clinical trials, the child participant and consent: A practical guide for investigators and sponsors," 2017.
[15] K. Singh *et al.*, "Mobile Health," in *Key Advances in Clinical Informatics: Transforming Health Care through Health Information Technology*. Elsevier Inc., 7 2017, pp. 183–196.
[16] "Australia: smartphone penetration rate 2017-2025 — Statista." https://www.statista.com/statistics/321477/smartphone-user-penetration-in-australia/
[17] "iOS - Health - Apple (AU)." https://www.apple.com/au/ios/health/
[18] "Glucose Buddy Diabetes Tracker." https://apps.apple.com/us/app/glucose-buddy-diabetes-tracker/id294754639
[19] B. M. Silva *et al.*, "Mobile-health: A review of current state in 2015," pp. 265–272, 8 2015.
[20] M. T. Baysari *et al.*, "Mobile Applications for Patient-centered Care Coordination: A Review of Human Factors Methods Applied to their Design, Development, and Evaluation," pp. 47–54, 8 2015.
[21] B. Qudah *et al.*, "The influence of mobile health applications on patient - healthcare provider relationships: A systematic, narrative review," pp. 1080–1089, 6 2019.
[22] C. E. Schairer *et al.*, "How could commercial terms of use and privacy policies undermine informed consent in the age of mobile health?" *AMA journal of ethics*, vol. 20, no. 9, pp. 864–872, 2018.
[23] M. Nouwens *et al.*, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," in *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery, 4 2020.
[24] C. Utz *et al.*, "(Un)informed Consent: Studying GDPR consent notices in the field," in *Proceedings of the ACM Conference on Computer and Communications Security*. Association for Computing Machinery, 11 2019, pp. 973–990.
[25] Y. O'Connor *et al.*, "Vision and voice in e consent: Future trends for health social networks," in *Procedia Computer Science*, vol. 141. Elsevier B.V., 2018, pp. 396–404.
[26] B. M. Bot *et al.*, "The mPower study, Parkinson disease mobile data collected using ResearchKit," *Scientific Data*, vol. 3, 3 2016.
[27] J. M. Radin *et al.*, "The healthy pregnancy research program: transforming pregnancy research through a researchkit app," *NPJ digital medicine*, vol. 1, no. 1, pp. 1–7, 2018.
[28] J. Wang *et al.*, "International researchkit app for women with menstrual pain: development, access, and engagement," *JMIR mHealth and uHealth*, vol. 8, no. 2, p. e14661, 2020.
[29] C. Lalloo *et al.*, "The icancope pain self-management application for adolescents with juvenile idiopathic arthritis: a pilot randomized controlled trial," *Rheumatology*, vol. 60, no. 1, pp. 196–206, 2021.