Abstract—My Health Record system is the Australian Government’s digital health record system that holds My Health Record. My Health Record is a secure online health record containing consumers’ health information. The system aims to provide health care professionals with access to key health information, e.g. listing medicines, allergies and key diagnoses; radiology and pathology test results. The system (previously named Personally Controlled Electronic Health Record) enables consumers to decide how to share information with any of their health care providers who are registered and connected to the system. The My Health Record system operates under the Australian legislative framework My Health Records Act 2012. The Act establishes, inter alia, a privacy framework specifying which entities can collect, use and disclose certain information in the system and the penalties that can be imposed on improper collection, use and disclosure of this information. This paper presents the formal specification (from the legislation) and verification of the My Health Record regarding how consumers can control who access the information, and how the system adheres to such access. We rely on the correct-by-construction Event-B method to prove control and access properties of the system.

Index Terms—Health records, Health records privacy, Formal specification and verification, Event-B

I. INTRODUCTION

The interest in introducing electronic personal health record systems has emerged as an important area of research in the medical and health informatics domain. These systems are indeed complex to understand, implement and use as they have many different components interacting to each other while managing sensitive information of their users. An electronic personal health record system is a digital version of a patient’s health information. The system makes patient’s information available instantly and securely to authorised users. Many countries have implemented their own system: the National Health Service implemented the Summary Care Record [1] in UK, ELGA [2] (Elektronische Gesundheitsakte) in Austria, the National Electronic Health Record [3] in Singapore, My Health Records [4] in Australia, among others.

In Australia, the first national electronic health record system was launched in 2012 [5], initially named Personally Controlled Electronic Health Record and later changed (in 2016) to My Health Record. The system is supported by a legislative framework. The objectives of the system were defined in the My Health Records Act 2012 (Cth) [1] by the Australian government as follows:

1. Help overcome the fragmentation of health information;
2. Improve the availability and quality of health information;
3. Reduce the occurrence of adverse medical events and the duplication of treatment; and
4. Improve the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers.”

The system is different from others implemented in other countries as its emphasis is to empower Australians through being able to personally control their health information: what is displayed and how others (e.g. GPs) can access such information. Consistent with this view, the government chose an opt-in model: users must register to use the system. However, the opt-in model did not achieve the expected number of users. It is reported that only 803 people registered in the first week, 4500 people in the first month, and as low as 6000 in the first two months all over Australia; while the targeted user number is 500000 within the first year of the operation of the system [5]. In 2019, the government adopted an opt-out model: all Australians were automatically registered and the decision of non-participating has to be specially requested by the individuals. This model has impacted the number of users of the system. My Health Record system (as in April, 2020) has 22.7M users, over 15.6M of them have data, around 1.95B health documents have been uploaded, and more than 90% of pharmacies, hospitals and service providers are registered [6].

Despite letting users to personally control their health information, they have no confidence on the system in terms of their privacy and who can actually access the information and how [7]–[9]. Privacy is addressed by having users choosing who can or cannot access their records. Access measures are addressed by having laws and regulation in place. However, there is not a clear way to ensure this to users. In this paper, we present a formal specification of the My Health Record system based on the legislation that defines it. We focused on the control and access properties of the health information. We also present the formal verification of such properties and the validation of the system (using animation of the
This paper is structured as follows. Section II introduces the formal methodologies and the mathematical notation used. Section III describes the My Health Record system and its requirements within the access and control framework. The formalisation of the system is introduced in Section IV. The section shows the formal specification and verification of the system in Event-B [10]. And the validation step, animation in ProB [11], and code generation, with EventB2Java [12]. Section V compares our approach with similar works. Finally, Section VI is devoted for conclusions and future work.

II. PRELIMINARIES

A. Event-B

Event-B [10] is a formal method technique to describe and analyse the behaviour of reactive systems. Event-B language is based on predicate logic and set theory. It includes a full-fledged battery of operations over sets and relations for modelling discrete software systems. Event-B models are composed of machines and contexts. Three basic relationships are used to structure an Event-B model, namely, a machine sees a context or can refine another machine, and a context can extend another context. Machines contain the dynamic parts of a model (i.e. variables, invariants, events), and contexts the static part of a model (i.e. carrier sets, constants). Events (after keyword events in Figure 1) are composed of two parts, the guard (the WHERE keyword in Figure 1) and the actions (the THEN keyword in Figure 1). Actions can only be executed if the guard holds. Each action determines how a machine variable evolves by modelling a variable assignment in Event-B (the := symbol). In Event-B, systems are typically modelled via a sequence of refinements. First, an abstract machine is developed and verified to satisfy whatever correctness and safety properties are desired. Refinement machines are used to add more detail to the abstract machine until the model is sufficiently concrete for hand or automated translation to code. Refinement proof obligations are discharged to ensure that each refinement is a faithful model of the previous machine, so that all machines satisfy the correctness properties of the original.

Figure 1 is an excerpt of the My Health Record system in Event-B. Machine abs_mch sees (keyword sees) context ctx_abs. The context is omitted in the figure; it defines two carrier sets (new data type) MY_HEALTH_RECORD modelling all possible record spaces in the system, and PEOPLE modelling all possible people of the system. Machine abs_mch defines three variables: my_health_report_DB, the set of all record spaces currently active in the system; consumer, the set of all users of the system; and MyHR, mapping consumers to their record space. MyHR is defined as a one-to-one function (↣). The possible values of variables is shaped by the invariant (after keyword invariants). Event opt_out models the action of a consumer c (after keyword ANY) to opt out the system. Consumers can opt out at any time, as long as they are part of the system (grd1). If the event is triggered, the consumer is removed from the set of active users (act1), as well as the consumer’s My Health Record (act2). To maintain consistency with the invariant (inv3), the mapping c↣MyHR(c) is removed from MyHR (act3). In Event-B, actions are executed in parallel.

Rodin [13] is an open source Eclipse based integrated development environment (IDE) for Event-B model development. The Rodin is a core set of plug-ins for project management, formal development, syntactic analysis, proof assistance and proof-based verification. Moreover, it comes with additional plugins to provide different functionalities and features: ProB [11] translates Event-B models to B to model finding, checking, deadlock and test case generation. It can also be used to animate the model; EventB2Java [12] is a code generator plugin that soundly generates JML-annotated Java code from Event-B. EB2ALL [14] is a plug-in that includes the EB2C, EB2C++, EB2J, and EB2C# plug-ins, each translating Event-B machines to the indicated language.

B. Mathematical notations

The following is the mathematical notation underlying our model. It is drawn from the Event-B notation [10].

1) Sets: Let S and T be sets and E and F expressions:
   - ∅ denotes the empty set.
   - S ∪ T is the set union.
   - S ∩ T is the set intersection.
   - S\{T = \{x | x ∈ S ∧ x \notin T\} is the set difference.
   - P(S) = \{x | x \subseteq S\}, the power set of S.
   - E → F is an ordered pair.
   - S × T = \{x → y | x ∈ S ∧ y ∈ T\} is the Cartesian product.

2) Set predicates: Let S, T and U be sets:
   - S ⊆ T denotes subset.
   - partition(U, S, T), S and T partition the set U, i.e. U = S ∪ T ∧ S ∩ T = ∅.
3) Relations: A relation is a set of ordered pairs; a many to many mapping. Let \( S \) and \( T \) be sets and \( r \) and \( p \) relations:
- \( \text{dom}(r) = \{ x \mid \exists y \cdot x \mapsto y \in r \} \) denotes the domain of \( r \).
- \( \text{ran}(r) = \{ y \mid \exists x \cdot x \mapsto y \in r \} \) denotes the range of \( r \).
- \( r \circ p = \{ x \mapsto y \mid \exists z \cdot x \mapsto z \in r \land z \mapsto y \in p \} \) denotes forward composition.
- \( S \join r = \{ x \mapsto y \mid x \mapsto y \in r \land x \in S \} \) denotes domain restriction.
- \( r \triangleright T = \{ x \mapsto y \mid x \mapsto y \in r \land y \in T \} \) denotes range restriction.
- \( S \triangleright id = \{ x \mapsto x \mid x \in S \} \) denotes the identity.
- \( r^{-1} = \{ y \mapsto x \mid x \mapsto y \in r \} \) is the inverse of relation \( r \).
- \( r[S] = \{ y \mid \exists x \cdot x \in S \land x \mapsto y \in r \} \) denotes relation image.

4) Functions: A function is a relation with the restriction that each element of the domain is related to a unique element in the range; a many to one mapping. Let \( S \) and \( T \) be sets:
- \( \rightarrow T = \{ r \mid r \in S \leftrightarrow T \land r^{-1}; r \subseteq T \triangleright id \} \) denotes partial function.
- \( \rightarrow T = \{ f \mid f \in S \rightarrow T \land \text{dom}(f) = S \} \) denotes total function.
- \( \rightarrow T = \{ f \mid f \in S \rightarrow T \land f^{-1} \in T \rightarrow S \land \text{ran}(f) = T \} \) denotes a bijective function; a one to one relation.

III. MY HEALTH RECORD SYSTEM

My Health Record system (herein MyHR) is an online centralised folder summary documents relating to the healthcare of consumers. The system is similar to a Dropbox folder\(^4\) where the health information of a consumer is summarised and can be accessed by different entities. The system aims to: improve consumers’ care, safety and medical communication. The lack of interoperability between hospitals and GPs is a common source of medical error. MyHR allows for health information to be in one place, which aims to avoid this problem; reduce the need to recite medical history. This reduces the need for consumers to explain (which could be wrong) their medical history; improve continuity of care between providers. Consumers often visit different service providers for the same condition. Having all health information consolidated in one single place might help GPs to continue a treatment.

The folder is mainly controlled by consumers, so, in principle, they can decide who can access which information. The system enables consumers to access their health information, add records (e.g. medication the consumer is taking), set privacy controls, hide or remove information and access another consumer’s MyHR (see nominated and authorised representatives below). This section introduces the system based on the Australian Acts My Health Records Act 2012 (Cth)\(^3\) and My Health Records Rule 2016 (Cth)\(^4\). The emphasis is on the control and access properties of the system. Figures\(^2\) and \(^5\) show the schematic representation of control and access of the different elements of the system. Figure 2 shows what can be controlled by the elements of the system. The ‘Type of’ arrow also indicates inheritance of permissions. For instance, a Restricted service provider is a type of General service provider. It can add restricted records as well as general ones. Figure 3 shows the access permissions to information. Similarly, the ‘Type of’ arrow also indicates inheritance of access. For instance, a Full access nominated representative can access both general and restricted records.

Fig. 2: Control scheme in MyHR

A. Definitions

Some of the definitions used throughout the paper are:

- **My Health Record**: the record of healthcare information that is created and maintained by the system operator in relation to the consumer.

- **My Health Record system (MyHR)**: a system for the collection, use and disclosure of healthcare information, in accordance to the consumer’s wishes.

- **Record**: information or an opinion about the health of a consumer. For instance, information about allergies, blood test results, medical conditions, prescriptions.

- **System operator**: a person in charge of establishing and maintaining the MyHR;

- **Consumer**: a person who has received, receives, or may receive healthcare. (Defined as healthcare recipient in the Act);

- **Service provider**: a registered entity that provides healthcare. (Defined as healthcare provider organisation or individual healthcare provider in the Act);

- **Nominated Representative**: a person appointed by the consumer (in agreement with the system operator) to access

\(^1\)Retrieved from www.dropbox.com
\(^2\)Retrieved from https://www.legislation.gov.au/Details/C2019C00337
\(^3\)Retrieved from https://www.legislation.gov.au/Details/F2016C00607
the consumer’s MyHR, in accordance to the consumer’s wishes.

**Authorised Representative**: a person (in agreement with the system operator) who has parental responsibility for a consumer aged under 14 or for a consumer who is not capable of making decisions for themselves.

**B. The system**

Consumers, once part of the system, are entitled to own only one MyHR; ownership cannot be shared. Initially, the MyHR is empty, no health information has been uploaded. Over time, the MyHR is populated with consumer’s health information (i.e., records), e.g., after a consumer visits their GPs, pharmacists or hospitals. A record is associated to only one MyHR and has only one owner: the owner of the MyHR where the record sits. Records can be marked as one of the following types:

- ‘general’: records that can be accessed by anyone with access permission to the MyHR. Records are marked ‘general’ by default;
- ‘restricted’: restricted records that need a special permission to be accessed;
- ‘hidden’: no one (including its owner) has access to these records. Consumers can recover them in agreement with the system operator.

Consumers can access their own records marked as ‘general’ and ‘restricted’. A key feature of the system is that consumers can add and delete records, and control which service providers and nominated representatives access what records.

Records will be marked as either ‘general’ or ‘restricted’. (General access permissions are included in the Restricted access permissions.) In addition, Restricted service providers can upload records to the MyHR. Records will be marked as ‘restricted’; Revoked service providers have access to no records.

Consumers can also be nominated or authorised representatives of someone else’s MyHR. A nominated representative can access or help manage consumers’ MyHR. They might be a family member, close friend or carer. Consumers can add or delete nominated representatives to their MyHR; they cannot nominate themselves. Similar to service providers, consumers can restrict the access of records to nominated representatives by assigning them to specific lists. A nominated representative can be in one of the following lists: General, Restricted or Full access. General nominated representatives can access all records of the MyHR marked as ‘general’; Restricted nominated representatives can access all records of the MyHR marked as ‘general’ and ‘restricted’. General access permissions are included in the Restricted access permissions; Full access nominated representatives are special Restricted representatives (thus, they have the same access permissions) with the additional capacity of uploading records to the MyHR. Records will be marked as either ‘general’ or ‘restricted’.

Consumers can also set an access code to their MyHR on their restricted records. If they want a service provider or nominated representative with General access to access restricted records, the consumer can provide the code.

An authorised representative is a person who manages the MyHR of someone who cannot manage their own. Hence, consumers cannot be authorised representatives of their own MyHR. An authorised representative might manage the record on behalf of a child, or an adult who lacks capacity. They are empowered under Australian law to do anything that the consumer would be able to do. The system operator is in charge of delegating authorised representatives to a consumer. Authorised representatives have full access and control over a MyHR as if they were the owners. Once a MyHR has at least one authorised representative, the owner of such MyHR loses all control over it. Table [I] summarises the properties of the system concerning access and control of the MyHR.

Access to the information can be bypassed in emergency situations. The *My Health Records Act 2012 (Cth)* defines where it may be permissible for entities to bypass the access controls. The Act defines an emergency access function, commonly referred as ‘break glass’ function. Such a function can be used when there is a serious threat to the individual’s life, health or safety and their consent cannot be obtained; or there are reasonable grounds to believe that access to the

---

3 The model in section IV does not consider this option as providing a General service provider or nominated representative with a code is semantically equivalent as granting them Restricted access.
Consumers can access their own records marked as 'general' and 'restricted'.

Restricted
Consumers can restrict access of service providers by listing them as operator.

HEALTH Consumers can add or delete nominated representatives to their Full access
Restricted
General Service providers have access to their consumers' health
Consumers can restrict access of nominated representatives by listing them as Full access
Restricted
General
Authorised representatives have full access and control over a
DB
threat to public health or safety of that person is necessary to lessen or prevent a serious
MyHR
MyHR

TABLE I: Control access properties of MyHR

| Property ID | Description |
|-------------|-------------|
| p1 (control) | Consumers can add, delete and restrict their own records. |
| p2 (access) | Consumers can access their own records marked as ‘general’ and ‘restricted’. |
| p3 (access) | Service providers have access to their consumers’ MyHR. |
| p4 (control) | Consumers can restrict access of service providers by listing them as General, Restricted or Revoked. |
| p5 (access) | General service providers with access to a MyHR can access all of the MyHR’s records marked as ‘general’. |
| p6 (access) | General service providers can also upload records to the MyHR. Records will be marked as ‘general’. |
| p7 (access) | Restricted service providers with access to a MyHR can access all of the MyHR’s records marked as ‘general’ and ‘restricted’. |
| p7.1 (access) | Restricted access permissions is a subset of General access permissions. |
| p8 (control) | Restricted service providers can also upload records to the MyHR. Records will be marked as ‘restricted’. |
| p9 (access) | Revoked service providers with access to a MyHR cannot access any record. |
| p10 (control) | Consumers can add or delete nominated representatives to their MyHR. |
| p11 (control) | Consumers can restrict access of nominated representatives by listing them as i.e. General, Restricted or Full access. |
| p12 (access) | General nominated representatives can access all records of the MyHR marked as ‘general’. |
| p13 (access) | Restricted nominated representatives can access all records of the MyHR marked as ‘general’ and ‘restricted’. |
| p13.1 (access) | Restricted access permissions is a subset of General access permissions. |
| p14 (access) | Full access nominated representatives can access all records of the MyHR marked as ‘general’ and ‘restricted’. |
| p15 (control) | Full access nominated representative can also upload records to the MyHR. Records will be marked as either ‘general’ or ‘restricted’. |
| p16 (control) | Authorised representatives have full access and control over a MyHR as if they were the owner. Once a MyHR has at least one authorised representative, the owner of such MyHR loses all control over it. |

IV. FORMAL MODEL IN EVENT-B

My Health Record system is composed of different elements that interact to each other. The model in Event-B introduces each element gradually in different machines (refinements). The abstract model contains a series of records marked as ‘general’, ‘restricted’ or ‘hidden’. The abstract model also defines consumers and the access to records, as well as the mechanisms for consumers to control the access. Finally, this machine introduces the system operators. The first refinement introduces service providers and their access to records. It also provides mechanisms for consumers to restrict service providers’ access. The second refinement introduces nominated representatives and the access mechanisms of nominated representatives to records. The final refinement introduces authorised representatives and how they control MyHR. Once a MyHR has an authorised representative, they act as owners of the system and the actual owner loses all control over the MyHR. Event-B models typically start with a very abstract machine and each refinement adds just as much information about the system. Due to space, the model present in this paper shows a more compact version of the original model (fewer refinements, but the same information). Both Event-B models (all POs discharged) can be found in [15]. Table II shows a description of each refinement. A more detailed description can be found in the coming subsections.

A. My Health Record system (abstract machine)

The abstract model defines the fundamental elements of the system:

- consumers. Healthcare recipients of the system;
- ‘break glass’ functionality is not modelled.

MyHR of that person is necessary to lessen or prevent a serious threat to public health or safety.\(^6\)


### Table II: Refinement strategy summary

| Machine | Summary |
|---------|---------|
| Abstract (section IV-A) | Health record, consumers, records and their categories: ‘general’, ‘restricted’ and ‘hidden’. |
| Refinement 1 (section IV-B) | Service Providers, their categories and their level of access to MyHR and records |
| Refinement 2 (section IV-C) | Nominated Representatives, their categories and their level of access to MyHR and records |
| Refinement 3 (section IV-D) | Authorised Representative and their level of access to MyHR and records |

- records. Consumers’ medical information. They can be categorised as ‘general’, ‘restricted’ or ‘hidden’; and
- My Health Record online space. It is owned by a consumer and it contains records.

The context of the model defines a new data type: PEOPLE, modelling potential users of the system, as well as potential system operators. Data type MY_HEALTH_RECORD models all possible My Health Record of the system. And data type RESOURCES models the possible records of the system. The machine defines variable my_health_record_DB ⊆ MY_HEALTH_RECORD, the set of all MyHR currently active. Variable consumer ⊆ PEOPLE defines the set of all users of the system. Variable MyHR ∈ consumer ⇒ my_health_record_DB maps consumers to their MyHR. It is defined as a bijective function as by definition a consumer owns exactly one MyHR, and each MyHR is owned by exactly one consumer. Variable system_operator defines the set of people (no consumers) that serve as system operators: system_operator ⊆ PEOPLE \ consumer. Records are the resources of the system containing medical information about a user; they are the elements to be shared. A record could be a blood test, hospital discharge summary, etc. (Our model does not distinguish between different records.). The model defines variable records ⊆ RESOURCES to represent the set
of records in the system. Variables \( \text{records}\_\text{mhr} \in \text{records} \rightarrow \text{my}_\text{health}_\text{record\_DB} \) and \( \text{consumer\_own\_records} \in \text{records} \rightarrow \text{consumer} \) are defined as total functions to guarantee that every record in the system is in exactly one MyHR, and has only one owner.

Variables \( \text{general}\_\text{records} \subseteq \text{records}, \text{restricted}\_\text{records} \subseteq \text{records}, \text{hidden}\_\text{records} \subseteq \text{records} \) are the set of records marked as ‘general’, ‘restricted’ and ‘hidden’, respectively. A record can be in only one of those categories. This fact is modelled as \( \text{partition}(\text{records}, \text{general}\_\text{records}, \text{restricted}\_\text{records}, \text{hidden}\_\text{records}) \). Consumers own all records on their MyHR:

\[
\forall r \mapsto c \in \text{consumer\_own\_records} \implies
\forall \text{mhr} \in \text{MyHR}, \quad c \mapsto \text{mhr} \in \text{MyHR}.
\]

We modelled the property via the following invariant

\[
\text{consumer\_own\_records}^{-1}.\text{records}\_\text{mhr} = \text{MyHR}.
\]

The model also defines events for the \( \text{control} \) of the elements in the \( \text{MyHR} \) (\( p1 \) (control)). Events \( \text{restrict}\_\text{record}, \text{general}\_\text{record} \) and \( \text{hide}\_\text{record} \) give owners of the \( \text{MyHR} \) the opportunity to control the category of each record. Event \( \text{unhide}\_\text{record} \) authorises a system operator to restore records which have been previously removed. Events \( \text{delete}\_\text{record} \) and \( \text{upload}\_\text{record} \) allow owners of the \( \text{MyHR} \) to delete and add records (respectively). Event \( \text{view}\_\text{record} \) defines the access of a consumer \( c \) to a record \( r \). As consumers can access their own records marked as ‘general’ and ‘restricted’ (\( p2 \) (access)), the event can be triggered only if the \( c \) owns \( r \) (\( r \mapsto c \in \text{records\_ownership} \)) and \( r \) is not marked as ‘hidden’ (\( r \notin \text{hidden\_records} \)).

Figure 4 depicts the event for marking a record as ‘restricted’ in the abstract machine. \( \text{restrict}\_\text{record} \) enables a consumer \( c \) to restrict record \( r \). The guard of the event establishes that \( c \) must have ownership over the record (\( \text{grd1} \)). If the event is triggered, record \( r \) is added to the list of records marked as ‘restricted’ (\( \text{act1} \)), and taken out from the list of general records (\( \text{act2} \)).

\[
\text{restrict}\_\text{record} \triangleq \text{ANY} \quad r \mapsto c
\]

WHERE

\[
\text{grd1} \triangleq r \mapsto c \in \text{records\_ownership}
\]

THEN

\[
\text{act1} \triangleq \text{restricted}\_\text{records} \leftarrow \text{restricted}\_\text{records} \cup \{r\}
\]

\[
\text{act2} \triangleq \text{general}\_\text{records} \leftarrow \text{general}\_\text{records} \setminus \{r\}
\]

END

Fig. 4: Event for marking a record as ‘restricted’.

B. Service Providers (refinement 1)

This model (which is a refinement to the model described in section [IV-A]) introduces service providers and their access to records in MyHR. The model defines a new data type \( \text{SERVICE\_PROVIDERS} \) modelling potential registered service providers. Variable \( \text{service\_providers} \subseteq \text{SERVICE\_PROVIDERS} \) defines the set of registered service providers in the system. Variable \( \text{consumer}\_sp \in \text{consumer} \leftrightarrow \text{service\_providers} \) maps consumers to service providers. It is defined as a relation to ensure that a service provider can be in charge of several consumers’ healthcare and a consumer can be associated with several service providers. Once a service provider is managing a consumer’s health care, such service provider has access (limited by the consumer’s will) to the consumer’s MyHR (\( p3 \) (access)). This is captured by variable \( \text{sp}_\text{MyHR}\_\text{access} \in \text{service\_providers} \leftrightarrow \text{my}_\text{health}_\text{record\_DB} \) that maps services providers to My Health Records, and predicate

\[
\forall c \mapsto sp \in \text{consumer}\_sp \implies
sp \mapsto \text{MyHR}(c) \in \text{access\_sp\_mhr},
\]

that is expressed in the model as the following invariant

\[
\text{access\_sp\_mhr} = \text{consumer}\_sp^{-1}.\text{MyHR}.
\]

Variables \( \text{general}\_sp\_list, \text{restricted}\_sp\_list \) and \( \text{revoked}\_sp\_list \) in the model map service providers to MyHR (\( \text{service\_providers} \leftrightarrow \text{my}_\text{health}_\text{record\_DB} \)). These variables modelled the General, Restricted and Revoked lists, respectively. By default, service providers are in the General list. A service provider can be in only one of the lists, this is modelled as \( \text{partition}(\text{sp}_\text{MyHR}\_\text{access}, \text{general}\_sp\_list, \text{restricted}\_sp\_list, \text{revoked}\_sp\_list) \).

Variables \( \text{general}\_sp\_access \in \text{service\_providers} \leftrightarrow \text{records} \) and \( \text{restricted}\_sp\_access \in \text{service\_providers} \leftrightarrow \text{records} \) model the level of access of service providers to records in MyHR. Service providers in General lists can access only records marked as ‘general’ (\( p5 \) (access)),

\[
\forall sp \mapsto r \in \text{general}\_sp\_access \implies r \in \text{general}\_records \land
sp \mapsto \text{records}\_\text{mhr}(r) \in \text{general}\_sp\_list.
\]

We express the property as the following invariant (notice that the access is not defined for service providers in the Revoked list (\( p9 \) (access)))

\[
\text{general}\_sp\_access =
\text{general}\_sp\_list: (\text{general}\_records \cup \text{records}\_\text{mhr})^{-1}.
\]

Service providers in Restricted lists can access records marked as both ‘general’ and ‘restricted’ (\( p7 \) (access)),

\[
\forall sp \mapsto r \in \text{restricted}\_sp\_access \implies r \in \text{general}\_records \cup \text{restricted}\_records \land
sp \mapsto \text{records}\_\text{mhr}(r) \in \text{general}\_sp\_list \cup \text{restricted}\_sp\_list.
\]

We express the property as the following invariant (notice that the access is not defined for service providers in the Revoked list (\( p9 \) (access)))

\[
\text{restricted}\_sp\_access = (\text{restricted}\_sp\_list:
(\text{general}\_records \cup \text{restricted}\_records) \cup \text{records}\_\text{mhr})^{-1})
\]

\[
\text{general}\_sp\_list: (\text{general}\_records \cup \text{records}\_\text{mhr})^{-1}
\]

\[
\cup
\]
To ensure that service providers with restricted permissions have also general permissions (p7.i (access)),
\[ \forall sp \mapsto mhr \in \text{general}\_sp\_list \implies sp \mapsto mhr \in \text{restricted}\_sp\_list, \]
we added the following invariant
\[ \text{general}\_sp\_access \subseteq \text{restricted}\_sp\_access. \]

The model extends the events from the refined machine for the control of the elements in the MyHR to update the new variables. New control events are introduced to enable consumers to assign service providers to General, Restricted and Revoked lists (p4 (control)). revoke_access_sp in Figure 5 shows the event for a consumer c to revoke the access of service provider sp to MyHR mhr. The guards of the event establish that c owns MyHR mhr (g\text{r}d1_\text{r1}), sp is in charge of c’s healthcare (g\text{r}d2_\text{r1}), and sp is not already in the Revoked list for that MyHR (g\text{r}d3_\text{r1}). If the event is triggered, the service provider sp is added to the Revoked list (act1_\text{r1}) and removed from the General or Restricted list (act2_\text{r1} and act3_\text{r1}). Access permissions for sp to mhr are also updated: sp cannot access any records in mhr (act4_\text{r1} and act5_\text{r1}).

\text{revoke_access_sp} \triangleq \text{ANY} sp \ mhr c

WHERE

\begin{align*}
g\text{r}d1_\text{r1}: & c \mapsto mhr \in \text{MyHR} \\
g\text{r}d2_\text{r1}: & c \mapsto sp \in \text{consumer}\_sp \\
g\text{r}d3_\text{r1}: & sp \mapsto \text{MyHR}(c) \notin \text{revoked}\_sp\_list
\end{align*}

THEN

\begin{align*}
\text{act1}_\text{r1}: & \text{revoked}\_sp\_list := \text{revoked}\_sp\_list \cup \{ sp \mapsto mhr \} \\
\text{act2}_\text{r1}: & \text{restricted}\_sp\_list := \text{restricted}\_sp\_list \setminus \{ sp \mapsto mhr \} \\
\text{act3}_\text{r1}: & \text{general}\_sp\_list := \text{general}\_sp\_list \setminus \{ sp \mapsto mhr \} \\
\text{act4}_\text{r1}: & \text{general}\_sp\_access := \text{general}\_sp\_access \setminus \{ mhr \} \\
\text{act5}_\text{r1}: & \text{restricted}\_sp\_access := \text{restricted}\_sp\_access \setminus \{ \{ mhr \} \} \\
\end{align*}

END

Fig. 5: Event for revoking access to a service provider.

The model also introduces new events for the access to records. Event view_record_service_provider enables a service provider to access a record. The event makes sure that the corresponding properties are not violating (e.g. a service provider in the General list can only access records marked as ‘general’). Events upload_general_record_SP and upload_restricted_record_SP enable service provider to upload general and restricted records, respectively, if they are allowed to do so (p6 (control) and (p8 (control))).

C. Nominated Representatives (refinement 2)

This model (which is a refinement of the model in section IV-B) introduces nominated representatives and their access permissions on records. The model defines variables general_nominated c consumer \leftrightarrow my\_health\_record\_DB, restricted_nominated c consumer \leftrightarrow my\_health\_record\_DB and full_access_nominated c consumer \leftrightarrow my\_health\_record\_DB to represent the lists of General, Restricted and Full access nominated representatives. Invariant general_nominated
\[ \cap \text{restricted}\_nominated = \emptyset \] ensures that a nominated representative is in either list (Full Access nominated are special Restricted nominated). Consumers cannot be nominated representatives of their own MyHR,
\[ \forall nr \mapsto mhr \in \text{general}\_nominated \cup \text{restricted}\_nominated \implies nr \mapsto mhr \notin \text{MyHR}. \]

We express the property as
\[ (\text{general}\_nominated \cup \text{restricted}\_nominated) \cap \text{MyHR} = \emptyset. \]

Variables general_nominated_access c consumer \leftrightarrow records and restricted_nominated_access c consumer \leftrightarrow records model the level of access of nominated representatives to records in MyHR. General nominated representative can access only records marked as ‘general’ (p12 (access)),
\[ \forall nr \mapsto r \in \text{general}\_nominated\_access \implies r \in \text{general}\_records \land \text{records}\_mhr(r) \in \text{general}\_nominated. \]

We express the property as
\[ \text{general}\_nominated\_access = \text{general}\_nominated \cap \text{general}\_records \setminus \text{records}\_mhr^{-1}. \]

Whereas Restricted nominated representatives can access records marked as both ‘general’ and ‘restricted’ (p13 (access)),
\[ \forall sp \mapsto r \in \text{restricted}\_sp\_access \implies r \in \text{general}\_records \cup \text{restricted}\_records \land \text{records}\_mhr(r) \in \text{general}\_sp\_list \cup \text{restricted}\_sp\_list. \]

We express the property as
\[ \text{restricted}\_nominated\_access = \text{restricted}\_nominated \cap (\text{general}\_records \cup \text{restricted}\_records) \setminus \text{records}\_mhr^{-1} \]
\[ \cup \text{general}\_nominated \cap (\text{general}\_records \setminus \text{records}\_mhr^{-1}) \]

Full access representatives have the same access permissions as Restricted representatives (p14 (access)),
\[ \forall nr \mapsto mhr \in \text{full}\_access\_nominated \implies nr \mapsto mhr \in \text{restricted}\_nominated. \]

We express the property as
\[ \text{full}\_access\_nominated \subseteq \text{restricted}\_nominated\_access. \]

To ensure that nominated representatives with Restricted level access have also General level access (p13.i (access)),
\[ \forall nr \mapsto r \in \text{general}\_nominated\_access \implies nr \mapsto r \in \text{restricted}\_nominated\_access, \]
we added the following property

\[
\text{general\_nominated\_access} \subseteq \text{restricted\_nominated\_access}.
\]

The model extends the events from the refined machine for the control of the elements in the MyHR to update the new variables. New events are introduced to enable users (owners) to add and delete nominated representatives (p10 (control)), as well as to control their level of access. Consumers are enabled to assign nominated representatives to General, Restricted or Full access (p11 (control)). Full access nominated can also upload records to MyHR. The model introduces events `upload_general_record_nominated` and `upload_restricted_record_nominated` that enable Full access representatives to upload records marked ‘general’ or ‘restricted’ (p15 (control)).

Event `grant_full_access_to_nominated` in Figure 6 shows the event for a consumer to grant Full access permissions to nominated representative in MyHR. The guards of the event establish that the consumer cannot be a representative of its own MyHR (grd1$_{r2}$), as the owner of the MyHR cannot be a representative of itself; (grd2$_{r2}$); and that is not already a representative nominated of MyHR (grd3$_{r2}$, grd4$_{r2}$ and grd5$_{r2}$). If the event is triggered, the nominated representative is added to both lists `restricted_nominated` and `full_access_nominated` (act1$_{r2}$ and act2$_{r2}$). As Full access nominated representatives are a special type of Restricted ones, access permissions of in mhr are also updated (act3$_{r2}$): n has access to all records in mhr that are marked ‘general’ and ‘restricted’.

\[
\text{grant\_full\_access\_to\_nominated} \triangleq \text{ANY n mhr c}
\]
\[
\text{WHERE}
\]
\[
\begin{align*}
\text{grd1}\_r2 & : c \neq n \\
\text{grd2}\_r2 & : c \not\in \text{MyHR} \\
\text{grd3}\_r2 & : n \rightarrow \text{mhr} \land \text{general\_nominated} \\
\text{grd4}\_r2 & : n \rightarrow \text{mhr} \land \text{restricted\_nominated} \\
\text{grd5}\_r2 & : n \rightarrow \text{mhr} \land \text{full\_access\_nominated}
\end{align*}
\]

\[
\text{THEN}
\]
\[
\begin{align*}
\text{act1}\_r2 & : \text{restricted\_nominated} \Rightarrow \text{restricted\_nominated} \cup \{n \rightarrow \text{mhr}\} \\
\text{act2}\_r2 & : \text{full\_access\_nominated} = \text{full\_access\_nominated} \cup \{n \rightarrow \text{mhr}\} \\
\text{act3}\_r2 & : \text{restricted\_nominated}\_access \Rightarrow \text{restricted\_nominated}\_access \cup \{(n) \times \text{dom(\text{general\_records}\_\text{\{\text{restricted\_records}\}_{\text{\{mhr\}}}})\}
\end{align*}
\]

\[
\text{END}
\]

Fig. 6: Event for granting full access to a nominated.

The model also introduces new events for the access to records. `view_record_nominated` enables a nominated representative to access a record. The event makes sure that the corresponding representation is not a nominated representation in the `Restricted` list can access records marked as ‘general’ and ‘restricted’.

D. Authorised Representatives (refinement 3)

This model (which is a refinement of the model in section IV-C) introduces authorised representatives and their access and control permissions on records and MyHR. Authorised representatives act as owners of the MyHR. The model defines variable `authorised_rep \in consumer \leftrightarrow \text{my\_health\_record\_DB}` that maps consumers with authorised privileges to MyHR, Consumers cannot be authorised representatives of their own MyHR,

\[
\forall c \leftrightarrow \text{mhr} \in \text{authorised\_rep} \Rightarrow c \not\in \text{MyHR}.
\]

We express the property as

\[
\text{authorised\_rep} \cap \text{MyHR} = \emptyset.
\]

If a MyHR has an authorised representative, the owner loses all control of the system, and the authorised representatives take over. The model captures this by adding a guard to each event that an owner can perform ensuring that such MyHR does not have any authorised representative (p16 (control)). As an example, guards for events `restrict_record` (in Figure 4), `revoke_access_sp` (in Figure 5), and `grant_full_access_to_nominated` (in Figure 6) are extended to hold also the following guard `MyHR(c) \notin \text{ran(authorised\_rep)}`: the owner of the MyHR can perform these actions only if the MyHR does not have an authorised representative.

E. Correctness of the model

We have proved the soundness of the model by discharging all proof obligations (POs) generated by Rodin. The model is composed of an abstract machine and 3 refinements. Our modelling resulted in 525 proof obligations, where about 77% (406) were discharged automatically using Rodin’s built-in provers. This high percentage of automation depends on the modelling style applied. For example, we added some redundant information (as variables in the model) to help provers in the verification process. For instance, variable `sp_MyHR_access`, in the first refinement, maps service providers to MyHR that they have access to. However, this information can be inferred from variables mapping service providers to records (general_sp_access and restricted_sp_access) – as records, by definition, belong to only one MyHR. The decision of adding this redundant information is that the model is self-explained and proof obligations are easier to discharge.

We have proved all properties described in Table II (and depicted in figures 2 and 3). That is to say, we have proved that the model lets:

- consumers have access and control over records (they can decide to mark them as ‘general’, ‘restricted’ or ‘hidden’);
- consumers have control over service providers. Consumers can list them as General, Restricted or Revoked;
- consumers have also control over nominated representatives. Consumers can add and delete, and list them as General, Restricted or Full access;
- authorised representatives to take full control of the MyHR;
- nominate representatives with Full access to upload records marked as ‘general’ or ‘restricted’;
- nominated representatives with Full access and Restricted permissions to access records marked as ‘general’ and ‘restricted’;
• nominated representatives with General permissions to access only records marked as ‘general’;
• service providers in the General list upload records marked as ‘general’, and access only records marked as ‘general’;
• service providers in the Restricted list upload records marked as ‘restricted’, and access records marked as both ‘general’ and ‘restricted’;

The correctness of a system not only depends on its verification (i.e. have we modelled the system right?), but also on its validation (i.e. have we modelled the right system?). As a validation step, we used two plug-ins of Rodin: ProB, to translate the model to B; and EventB2Java, to generate JML-annotated Java code from the model. ProB can be used as an animator of the specification. The animation in ProB is fully automatic. We animated our model in ProB finding no inconsistencies; adding a level of confidence on the model. We also used the EventB2Java tool to translate the last refinement of the model. The Java implementation of MyHR consists of 48 Java classes. There is a Java class that implements JUnit test cases: 30 test cases manually written that conform to the My Health Record specification. The implementation passed all tests. Both the ProB animation and the description of the test cases (along with the implementation) can be found in [15].

V. RELATED WORK

There are as many different models of online health record systems around the world as there are healthcare systems. There are also many different approaches implemented by different countries that have been designed based on their own policy frameworks. In United Kingdom, the National Health Service implemented the Summary Care Record [1] (SCR). A SCR is an electronic consumer record that contains health record information. Once a consumer is registered with a GP, then the consumer’s SCR is created automatically (consumers can opt-out). Records in the system cannot be fully deleted, although consumers can request for their information to be withheld from the system once opted out. SCRs can be accessed by service providers’ stuff (as long as they are in charge of the consumer’s healthcare and they access the information through a secure system). In Austria, ELGA [2], [16] (elektronische Gesundheitsakte) is an information system that provides consumers and their healthcare entities with an access to their health records. Health records are created at various health facilities. ELGA networks the data and makes it available electronically. The system is available to everyone who is covered by the Austrian health care system, and it enables consumers to opt out. In Singapore, the National Electronic Health Record [3] (NEHR) is a secure online system that collects summary of consumers health records across different service provider providers. This enables authorised healthcare professionals to have a holistic picture of your healthcare history.

These systems have similarities to MyHR. The key feature of MyHR, and difference w.r.t. to other systems, is that consumers have access to and can fully control what is stored on their systems. They can also decide which service providers and nominated representatives can access which records. A similar system is the one developed in Estonia. The Electronic Health Record system [17] (e-Health Record) creates a common record every consumer can access online. Every Estonian is automatically included in the system from birth, and they are enabled to opt out at any time. In e-Health Record, consumers can restrict records from service providers, they can also grant access to other consumers (i.e. nominated representatives). Unlike MyHR, consumers cannot delete any records nor upload information (e.g. blood sugar values). Furthermore, no formal specification and verification has been performed on these systems.

Our work closely follows Role Based Access control [18], [19] (RBAC), which is a classic access model that uses the notion of users, roles and defines the privileges between those notions. Users (e.g. service providers) might have specific roles (e.g. General access) that define how to access resources (e.g. general service providers can only access records marked as ‘general’). Formalisation of RBAC has been done in Z [20] and in B [21]. We inspired our work on these works, although, the work present in this paper is shaped by a specific domain following specific policy frameworks. SGAC [22] is a healthcare access control model that manages the access to consumers’ records. The model has been formally verified with Alloy [23] and ProB [11]. Our work is similar to SGAC as it is the specification and verification of a health record system. However, the target specification language is different: we used Event-B and the associated tools for verification and code generation. Furthermore, unlike SGAC, the specification present in this paper is not the specification of an ideal system rather a realistic one. We present a specification that closely follows the legislative framework that defines the system, without making any assumption. As a future work, we plan to incorporate some of the SGAC features, e.g. more fine grained access to records and conflict resolution, as these enhance MyHR. eXtensible Access Control Markup [24] (XACML) is an attribute-based access control standard. It evaluates access requests according to rules. A rule has a subject (e.g. a service provider), an action (e.g. access), a resource (e.g. a record), and a effect (permit or deny). The standard has been formalised in CSP [25] and VDM [26]. XACML can be used for MyHR, but the standard does not natively support inheritance of permissions (e.g. Restricted permissions inherit General permissions). Azeem et al. [27] present a specification of an e-Health system in Z. The system deals with the scheduling of GPs and patients. Their work has the same spirit as the one in this paper (even though the system is different). However, we present not just the specification, but also the verification of the system and its validation.

VI. CONCLUSION

Electronic personal health record systems play a key role in today’s society. The benefits are clear: avoids healthcare fragmentation and duplication; supports accessibility and availabil-
ity, allowing timely and instantly access to information; improves coordination and quality of service providers; improves readability and accuracy, reducing misinterpretation; among others. No wonder why it is one of the 14 Grand Challenges for Engineering in the 21st Century.[28] These systems contain sensitive and confidential health information about consumers. As such, it is imperative to make sure that the right mechanisms for control and access are in place. Not just to ensure that health information is properly managed (which is of paramount importance), but also for users to gain confidence in the system: it would be useless if users did not trust it. This paper presents the formal specification and verification of the My Health Record System, the electronic personal health record system being used in Australia. We retrieved a set of control and access properties from the Australian legislation that defines the system. We formally modelled the system and its properties in Event-B and proved it correct. As a validation step, the model was animated by translating it to ProB. This gave us a layer of confidence in the model. We then generated JML-annotated Java code from the Event-B model and manually implemented JUnit test cases that conform to the system specification. An advantage of testing the specification is that it is done in terms of the application domain; on a much higher abstract level. Therefore, tests are relevant, as they exercise user needs and requirements, taking the system as a whole.

Work in progress is aimed at (i) proposing a more fine-grained mechanism for accessing health information, so users are able to control not just how to disclose health information to service providers, but also to GPs within those service providers: (ii) opening an avenue for using formalism to verify legislation. Formal modelling and the need to make abstractions and refine them, help understand the system, while finding inconsistencies in it. As future work, we plan to formally model the Act that defines the regulations for physical health records and formally prove the consistency between the legislation and MyHR.

REFERENCES

[1] N. H. S. Digital. (2020, May) Summary Care Records (SCR). Accessed, June 2020. [Online]. Available: https://digital.nhs.uk/services/summary-care-records-scr

[2] ELGA. My electronic health records. Accessed, June 2020. [Online]. Available: http://www.elda.gov.at/en/about-elda/

[3] HHS. (2020) National Electronic Health Record (NEHR). Accessed, June 2020. [Online]. Available: https://www.hhs.gov/nh/neh/home

[4] A. D. H. Agency. My Health Record (MyHR). Accessed, June 2020. [Online]. Available: https://www.myhealthrecord.gov.au

[5] J. Xu, X. Gao, G. Sorwar, and P. Croll, “Implementation of E-health Record Systems in Australia,” The International Technology Management Review, vol. 3, pp. 92–104, 2013. [Online]. Available: https://doi.org/10.2991/itmtr.2013.3.2

[6] M. H. Record, “Statistics and Insights,” April 2020. [Online]. Available: https://www.myhealthrecord.gov.au/sites/default/files/scr/1213_stats_april_2020_v2.pdf?159076530 Accessor, June 2020.

[7] N. E.-H. T. A. (nehta). (2011, April) Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system . Accessed, June 2020. [Online]. Available: https://www.privatehealthcareaustralia.org.au/wp-content/uploads/PCEHR-Draft-Concept-of-Operations2.pdf

[8] T. Patten. (2019, April) A Healthy Dose of Caution: An Analysis of Australia’s My Health Record. Accessed, June 2020. [Online]. Available: https://www.bakermckenzie.com/en/insight/publications/2019/04/a-healthy-dose-of-caution

[9] D. Lupton, “Id like to think you could trust the government, but I don’t really think we can’: Australian women’s attitudes to and experiences of My Health Record,” DIGITAL HEALTH, vol. 5, p. 20552076/19847017, 2019, pMID: 31069106. [Online]. Available: https://doi.org/10.1177/2055207619847017

[10] J.-R. Abrial, Modeling in Event-B: System and Software Engineering, 1st ed. New York, NY, USA: Cambridge University Press, 2010.

[11] M. Leuschel and M. Butler, “ProB: A Model Checker for B,” in FME 2003: Formal Methods, K. Araki, S. Gnesi, and D. Mandrioli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 855–874.

[12] V. Rivera, N. Catano, T. Wahlis, and C. Rueda, “Code Generation for Event-B,” International Journal on Software Tools for Technology Transfer, January 2015. [Online]. Available: https://www.researchgate.net/publication/274036119_Code_Generation_for_Event-B

[13] J.-R. Abrial, M. Butler, S. Hallerestede, T. S. Hoang, F. Mehta, and L. Voisin, “Rodin: An Open Toolset for Modelling and Reasoning in Event-B,” Int. J. Softw. Tools Technol. Transf., vol. 12, no. 6, p. 447466, Nov. 2010.

[14] D. Mery and N. K. Singh, “Automatic Code Generation from Event-B Models,” in Proceedings of the Second Symposium on Information and Communication Technology, ser. SoICT 11. New York, NY, USA: Association for Computing Machinery, 2011, 2. p. 179188. [Online]. Available, https://doi.org/10.1145/2069216.2069225

[15] V. Rivera, "My Health Record formal model." https://github.com/varivera/mhr commit: b04e92babae61e4f845c55d51614e45a044224, 2020.

[16] S. Herbek, H. Eisl, M. Huch, A. Scharer, S. Sabutsch, G. Rauchegger, A. Kollmann, T. Philipp, P. Dragon, E. Seitz, and S. Repas, “The Electronic Health Record in Austria: a strong network between health care and patients,” European Surgery, vol. 44, 06 2012.

[17] Healthcare. e-health records. Accessed, June 2020. [Online]. Available: https://e-estonia.com/solutions/healthcare/e-health-record/

[18] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-based access control models,” Computer, vol. 29, no. 2, pp. 38–47, 1996.

[19] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, Role-Based Access Control, 2nd ed. USA: Artech House, Inc., 2007.

[20] D. Power, M. Slaymaker, and A. Simpson, “On Formalizing and Normalizing Role-Based Access Control Systems,” The Computer Journal, vol. 52, no. 3, pp. 305–325, 2009.

[21] N. Huynh, M. Frappier, A. Mammar, R. Lakloue, and J. Desharnais, “Validating the RBAC ANSI 2012 Standard Using B,” in Abstract State Machines, Alloy, B, TLA, VDM, and Z. Y. Atit Amour and K.-D. Schewe, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 255–270.

[22] N. Huynh, M. Frappier, H. Pooda, A. Mammar, and R. Lakloue, “SGAC: A Multi-Layered Access Control Model with Conflict Resolution Strategy,” 05 2019.

[23] D. Jackson, Software Abstractions: Logic, Language, and Analysis. The MIT Press, 2006.

[24] OASIS. (2013, January) Extensible Access Control Markup Language (XACML) Version 3.0. Accessed, June 2020. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[25] J. Bryans, “Reasoning about XACML Policies Using CSP,” in Proceedings of the 2005 Workshop on Secure Web Services, ser. SWS 05. New York, NY, USA: Association for Computing Machinery, 2005, p. 2835. [Online]. Available: https://doi.org/10.1145/1103022.1103028

[26] J. W. Bryans and J. S. Fitzgerald, “Formal Engineering of XACML Access Control Policies in VDM++”, booktitle="Formal Methods and Software Engineering," M. Butler, M. G. Hinche, and M. M. Larrondo-Petrie, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 37–56.

[27] M. W. Azeem, M. Ahsan, N. M. Minhas, and K. Noreen, “Specification of e-Health system using Z: A motivation to formal methods,” in International Conference for Convergence for Technology-2014, 2014, pp. 1–6.

[28] NAE. (2020) National Academy of Engineering, 14 Grand Challenges for Engineering (Advance Health Informatics). Accessed, June 2020. [Online]. Available: http://www.engineeringchallenges.org/8938.aspx