applied sciences

MDPI

Article

Privacy-by-Design and Minimization within a Small Electronic Health Record: The Health360 Case Study

Raffaele Conte [1], Francesco Sansone [2], Alessandro Tonacci [2,*] and Anna Paola Pala [2]

[1] National Research Council of Italy (CNR), Piazzale Aldo Moro 7, 00185 Rome, Italy
[2] Institute of Clinical Physiology, National Research Council of Italy (IFC-CNR), Via Moruzzi 1, 56124 Pisa, Italy
* Correspondence: atonacci@ifc.cnr.it; Tel.: +39-050-3152350

Abstract: Electronic health records are playing an important role in todays' clinical research, with the possibility to collect a wide amount of data from different sources, not only within a structured clinical setting, but also making best use of new portable technologies, such as smartphones, sensors and Internet-of-Things, as an unprecedented spring of data. In this way, even in small clinical centers, often featuring limited financial availabilities, not only clinicians can have a complete, timely outlook on patients' health, but also data scientists could use such information to build and train tailored models in the broader perspective of "p4 medicine". However, all this should align with the strict regulations and needs concerning data privacy and security, safeguarding the rights of the individual and the confidentiality of information related to their healthcare status. Here, we present a case study dealing with Health360, a platform designed to fill in this gap, representing the ideal solution for small clinical centers, where usability and cost-affordability are key characteristics for such a system, to collect multimodal data from various sources actually employed in the framework of neuromuscular conditions. The platform, designed under the Software-as-a-Service paradigm, actually collects data from different clinical centers active in the field of neuromuscular diseases, and therefore was designed to grant access to the data to specific professionals depending on their roles. At the same time, to the benefit of data scientists, Health360 enables joint data processing, with the management of authorization principles for various health professionals from different clinical centers, which is regulated by the data minimization principle, based on the accessing profile. Under such premises, we present here the approach followed for the implementation of the platform, managing the trade-off between the need from various professionals for accessing the complete dataset and the privacy requirements, as well as confidentiality maintenance for sensitive data of patients enrolled on the project.

Keywords: access; data protection; electronic health record; GDPR; healthcare; minimization; privacy; SaaS; security

Citation: Conte, R.; Sansone, F.; Tonacci, A.; Pala, A.P. Privacy-by-Design and Minimization within a Small Electronic Health Record: The Health360 Case Study. *Appl. Sci.* **2022**, *12*, 8441. https://doi.org/10.3390/app12178441

Academic Editor: Alexander Barkalov

Received: 27 June 2022
Accepted: 23 August 2022
Published: 24 August 2022

1. Introduction

In the framework of data science, the collection of wide amounts of data progressively becomes more critical. Thanks to the advancements of Information and Communication Technologies (ICT), nowadays large datasets regarding the universe of healthcare and well-being are made available, merging together data from clinical settings and information coming from personal devices, including smartphones; biomedical sensors, such as wearables; home automation systems, including Internet-of-Things (IoT); and so forth [1,2].

In the last decades, this scenario has attracted the major players of the ICT field, including Apple, Google, Amazon and Microsoft, making them develop and provide solutions, available via Smartphone, aimed at research and care (i.e., the development frameworks Apple HealthKit and Research Kit or Google Fit) [3,4].

This leads to a noteworthy asset for the data scientist that should be treated with care, taking into account the authorizations and limitations concerned with the privacy of data and the safeguarding of patients and individuals whose data are being treated [5,6].

Within such an, often narrow, edge, the software developers operating within the healthcare universe should play their efforts, with attention devoted to patients' data protection and privacy, and at the same time to the optimization of benefits for the clinician, the data scientist and the scientific community at large.

At the same time, there is an increasing need, from the clinical centers, to use ICT-based solutions for the agile collection of personal and clinical data. Indeed, several clinical centers, even in technologically advanced countries, still make large use of pen-and-paper clinical data reports, thus resulting in high costs and burden to clinical personnel, especially when dealing with longitudinal data [7]. As such, there is mounting evidence about the advantages of technological support for collecting data [8], driving clinicians to ask for new approaches to their everyday practice.

However, not all clinical centers have the possibility to take advantage of complex, exhaustive, well-grounded electronic health records, developed by main international players in the specific sector. This drives many of them to adopt simplified tools, often specifically tailored to one or to a limited group of functionalities, combining ease of use and cost-affordability [9].

The solution presented here, named "Health360", able to collect data from a patient or an individual concerning their health at 360 degrees, was developed to fill in this gap. Indeed, it represents a cost-effective, easy-to-use solution aimed at collecting and merging data from clinical centers and/or in research projects about many different clinical fields. All this including an eye to simplify the duties of the clinicians in collecting and storing data, and the other one to provide the data scientist with organized records to implement advanced computational models to retrieve relationships between clinical and instrumental variables, as well as between a genotype and phenotype of a given condition or group of diseases [10].

2. The Health360 Framework

Health360 is a software application, accessible through "WWW", defined as a "framework" since it constitutes a shared, scientifically valid basis, to implement and customize a managerial tool, which is efficient, multi-standard, representing the pivotal item of analysis and management of clinical and health-related data, available in scenarios such as hospitals, health residences or even sport clubs. It was developed under the Software-as-a-Service (SaaS) paradigm, therefore as a cloud-based software solution.

Overall, the tool should be capable of managing in a complete, integrated manner, all clinical and instrumental data, overcoming the actual limitations of different management software tools, representing a problem for clinicians in terms of an integrated information reading and interpretation. Indeed, several software solutions are limited in terms of their adaptability to the users' needs or, conversely, are even too flexible but extremely complex and difficult to be understood and practiced by clinical staff. Therefore, Health360 employs the most recent ICT technologies to obtain a product that will be flexible enough to be adapted to different situations, maintaining an excellent ease of use, thanks to its capability to build up the system with the strictly necessary modules for a given activity and scenario.

2.1. The Health360 Architecture

The Health360 application was built based on two levels: a "front-end", which is also used to implement the user interface (UI), aggregating data obtained by the distributed "back-end" (Figure 1). The framework was developed aimed at obtaining a modular, distributed architecture, featuring a back-end composed of several modules, eventually distributed within a network, able to communicate with each other and share data. Therefore, the concept is to pick up data at the source and to aggregate them "on-demand". Thus, data sources are authoritative for particular data, since they generate the data themselves,

to limit the data duplication within a central repository, with a consequent synchronization and related incongruence risk. The network becomes part of the database, whereas the data aggregation is managed by the application.

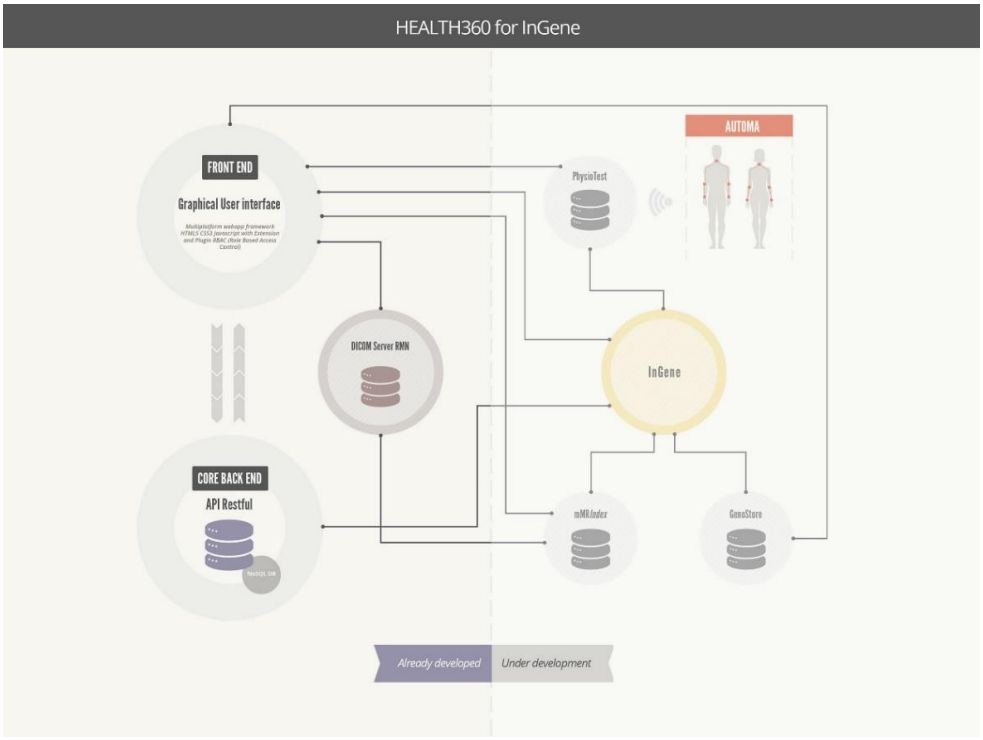

Figure 1. Basic architectural overview of a sample scenario for Health360.

Under such premises, the system architecture was built under the REST paradigm, using the HTTP protocol, according to the API-first approach, firstly allowing the design and the development of the Application Program Interface (API) as the application back-end and, just after the remaining parts, the front-end is developed [11].

The advantage for such an approach relies on the fact that, on a single back-end, it is possible to build up several front-ends for different devices (e.g., a web-app, a mobile app, and eventually a tablet-based mobile app).

Concerning data storage, in order to have a flexible tool for the attributes managed, NoSQL databases are used, including MongoDB and Redis, allowing higher flexibility in creating and managing data structures, and ensuring high performances using alternative data models with respect to the typical relational model [12].

Being conceived as a Software-as-a-Service, the application relies on an infrastructure capable of managing it through virtual machines and containers, making it a cloud-native application, with several advantages. To create the application, PHP was used, being particularly useful to develop web-apps, with the Symfony framework, according to the Model-View-Controller (MVC) pattern, commonly adopted in object-oriented programming languages [13,14].

The back-end is made up of a "core" module, capable of managing the personal data of an individual, their anamnesis and risk factors, the contact sessions with the organization and the examinations, even though future adjustments in this regard are still possible to further enhance privacy and security of data. Other data sources (RIS-PACS, screening archives, informative systems for laboratory medicine, etc.) are seen as further back-ends, eventually available depending on the use case. Then, the front-end will retrieve the information from the different back-ends and aggregate them in real-time. The application user interface was developed to be responsive, so to adapt to the screen size of the device used (a PC or a tablet). This characteristic is particularly useful to offer the best user

experience regardless of the tool employed, that could be eventually different depending on the use scenario.

2.2. Use Case: Health360 Applied to Neuromuscular Diseases

The Health360 framework is mainly used as an integrated tool for managing and analyzing data within the field of neuromuscular disorders. Actually, the end-users of this tool include four clinical partners located in Tuscany Region, Italy, which represent the core for research and clinical care in the related field in the area.

Overall, neuromuscular diseases require careful study concerning the genotype–phenotype association, in order to understand the precise characteristics of each individual affected by such conditions, and to adapt a personalized therapy, maximizing its result [15]. Therefore, the need emerges to collect various kinds of data, including those from genetics, muscular diagnostics, physiotherapy, and cardiovascular exams, to support the clinician in drawing a complete framework about the health condition of the patient, in defining treatment plans and in monitoring the disease course. This scenario is completely integrated with the concept of precision medicine, where the aim is to look for a therapy with maximum efficacy, based on correlation analysis between clinical and genetic data within a patient.

This is particularly important within the field of neuromuscular diseases, particularly those defined as "rare", where a specific syndrome is present just in a very small number of individuals. In this scenario, the typical approach, based on randomized cohorts to assess the efficacy of a given treatment (either a pharmacological one or not), is often inadequate, due to the low number of individuals composing the cohorts. Therefore, the concept of precision medicine in this domain is particularly appreciated, also thinking about the plethora of different rare neuromuscular diseases known to date, taken together accounting for thousands cases worldwide.

The first step in this process is represented by the diagnostic phase, particularly critical as several symptoms are common, or slightly different, between conditions. Therefore, being able to distinguish similar features, which are slightly variable between pathologies, is particularly helpful to clinicians to draw an appropriate diagnosis, avoiding potentially critical issues in this phase, which could make the whole therapeutic process vain.

Within the field, Health360 is mainly used to collect data from Becker and Duchenne muscular dystrophies but can potentially host data from other clinical conditions.

More specifically, in the light of the modular concept for the platform above mentioned, several modules were developed, as indicated below:

- PhysioTest: It allows for the administration of physiotherapy assessments through personalized user interfaces for specific tests, including Performance of Upper Limb (PUL), Six-Minute Walk Test (6MWT), Motor Function Measure (MFM), and North Star Ambulatory Assessment (NSAA) [16].
- NeuroExam: It was developed to execute neurological examinations [17].
- GenoStore: It stores the patient's genotype to study and selects individuals with particular genetic variants.
- MRIndex: It integrated muscular Magnetic Resonance Imaging and, by applying a segmentation algorithm, it provides a score for the subcutaneous fat infiltration within the muscular tissue, as an indicator of the muscular involvement within the clinical condition [18].
- PhenoLink: It allows for navigation within Human Phenotype Ontology (HPO), a biomedical ontology allowing the user to define, in a coded manner, a patient's phenotype.
- InGene: It enables selecting different parameters, by filtering or highlighting personal attributes, clinical test results, and so forth. It applies such parameters to statistical analysis in selected patients, through multivariate techniques, to highlight clusters of individuals based on the genotype–phenotype correlations. It represents a useful tool in clinical research, supporting diagnostic and care plan personalization [19].

3. Normative Aspects of an SaaS Platform

Nowadays, the paradigm of the software solution fruition has changed, due to the devices used every day for work or leisure. In fact, the use of smartphone or tablet devices has grown recently, so that the software applications and tools should be usable on such devices and on their screen rather than on personal computers. At the same time, it is necessary to maintain the documents produced by such devices in accessible, safe, secure spaces, guaranteeing the data integrity. Therefore, large cloud-based storage facilities need to be implemented, together with the possibility to allocate computational resources in cloud, too.

Under such premises, it is then evident that normative aspects need to be carefully considered when talking about cloud services, and SaaS in particular, as explained below.

3.1. Usability and Accessibility

Usability and accessibility are key for an application, especially when considering a smartphone app, being downloaded and eventually uninstalled in a very short amount of time, in case they do not meet the requirements of the end-user. This concept is also important, albeit less disruptive, in other software tools, including SaaS. In this regard, one of the most widely used models is the "freemium", featuring basic functionalities free of charge, and delivering advanced functions just after the payment of a fee. This approach allows the user to evaluate the "core" functionalities of the application without needing to spend money blindly.

Usability is one of the eight quality characteristics for a software according to the ISO/IEC 25010 standard, the other ones being: functional suitability, performance efficiency, compatibility, reliability, security, maintainability, and portability. Usability is defined as the property of an object to be easily understood, used and appreciated by the end-user. Therefore, a usable software product should be adequate to the needs of the end-user, and meet his/her expectations, with intuitive functioning, easy to be understood and esthetically pleasant.

In developing the user interface, the popular Nielsen heuristic have been employed, in order to optimize the user experience and interaction with the tool, overall.

As such, all the national and European rules and guidelines for usability have been taken into account for the development of Health360, including the ISO/IEC 25010 standard above mentioned, the EN 301 549 European standard for digital accessibility [20], specifying requirements for ICT to be accessible for people with disabilities, the latter giving birth to the Directive (EU) 2016/2102—accessibility of websites and mobile applications of public sector bodies, in turn received by the national regulations in Italy (Law Decree 2018/106) [21].

Specifically, in the design and development of Health360, the usability was leveraged, taking into account that software should be used in particular scenarios, such as the one represented by a clinical laboratory, or within the development of tricky tests, such as neurological examinations, or even in outdoor scenarios, such as the experimental setting where the 6MWT occasionally takes place, in some clinical institutions. As such, the 6MWT user interface features the accessibility directly with the operator's thumbs for any key button exposed (Figure 2). Furthermore, as Health360 is also used on mobile devices, in the user interface development, the available space to visualize information was taken into account. As such, some functionalities selectively hiding or exposing some information and sections when needed or not needed were included.

Figure 2. The 6MWT basic user interface.

3.2. Contract of Use, Informative Obligations and Service Levels

An SaaS application sees a slightly different contract of use with respect to traditional applications (those installed within an own device). Nowadays, since many of the SaaS market players are big ICT companies, it is required to accept the contract proposed in order to use the platform. Otherwise, when SaaS applications are provided by small factories, it is still possible to define a specific contract between the parts, since this approach could eventually provide mutual advantages for both the developer and the user.

In general terms, an SaaS application, when using personal data, as in the case of Health360, requires a specific explicit contract between the parts, at least concerning the personal data treatment person-in-charge, since the provider could be required to be qualified as the processor for personal data in agreement with Article 28 of EU Regulation 2016/679 (GDPR). Basically, when possible, the definition of a contract between provider and user organization (B2B), or between the provider and single consumers (B2C) should be preferred, but its possibility largely depends on the specific situation. Cloud contracts go under the regulations of ordinary contracts, observing general discipline and what is eventually agreed between the parts. In case some aspects are not defined, it needs to comply with more similar contract types, including services contracts and licensing contracts.

A cloud contract falls in the category common law contracts, requiring a set of definitions and, usually, several documents or sections where the modality of service providing (Terms of Service) is defined, together with the service levels (Service Level Agreement), for the provider, the Privacy Policy related to personal data treatment, and the Acceptable Use Policy, that is to say the indications about how the user is engaging themselves in the service use. The latter document is pivotal to the provider as it excludes own responsibility in case of improper service use by the user. Interestingly, among these, Terms of Service could also indicate a compensation, not necessarily a payment, for service provision.

However, cloud solutions providers should comply with the 2000/31 Directive for electronic commerce, and with the 2011/83 Directive for consumers' rights, received by national regulatory organisms, therefore Health360 is regulated, under these aspects, by the Italian law.

A particularly critical aspect for SaaS services is related to the right of withdrawal. Usually, the consumer has 14 days to exert the right of withdrawal starting from the day of

contract signing once all the relevant information is received. However, with cloud services, and with SaaS applications, this time window could, in some instances, be enough even to take advantage of the whole service offered (for example, in an e-learning based course or similar cases). In such cases, it is possible that the right of withdrawal is excluded when the complete service fruition is performed.

A particularly critical aspect is related to data ownership. This feature is quite clear in cases of personal data, whereas in the case of non-personal data elaborated from those inserted within the cloud platform by the user, it should be faced with particular attention. In fact, they are not necessarily owned by the user, since they come from data inserted by the user but, at the same time, they are either explicitly (through analytic functionalities of the platform) or implicitly (through log data) produced by the platform, whose ownership is the provider's, in turn possibly claiming the data ownership for their effective use. In the case of Health360, since its commercial use is not yet foreseen, and being the platform used within research projects, its use and results' intellectual property are regulated by agreements signed between the parties before the project takeoff.

3.3. Ethical Aspects in Machine Learning and Artificial Intelligence

Given the recent massive use of Machine Learning and Artificial Intelligence (AI) in the scientific universe and particularly within SaaS applications, related ethical aspects cannot be deemed as juridical aspects; however, the use of such technologies carries legal consequences. Health360 is also involved in this kind of discussion, as planning to use Machine Learning, particularly in the InGene module mentioned some paragraphs before, is occurring in several SaaS applications.

Such technologies still include several critical aspects, including biases, during the learning phases, leading to lower reliability of the results obtained. In addition, many of these solutions, particularly those relying on the Deep Learning methodologies, are still a sort of black box for users, making them difficult to be employed in a medical framework, where they are still never applied as a diagnostic tool.

Such an idea finds a juridical counterpart in the EU GDPR 2016/679 Regulation, where Article 22 states that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them". In light of that, the AI use is not limited, but what is limited is taking decision exclusively based on AI solutions.

Surely, AI-based solutions will play a major part in the near future within the development of human enhancing technologies, especially when combined with biotechnologies, medical, biomedical and genetic sciences; however, such a perspective is still under study from lawyers and sector experts seeking new models to optimally manage such processes, particularly in the identification of key responsibilities.

4. Data Treatment

As said, the treatment of both personal and non-personal data is particularly critical in all software solutions complying with the SaaS model, and noteworthy in the Health360 platform, for managing clinical and genetic data. The main criticisms in this respect concern roles of data processing, lawfulness, purposes, minimization principle, technical and organizational measures, and data protection impact assessment (DPIA).

The GDPR 2016/679 Regulation [22] now changes the perspective concerning data processing with respect to the past, aiming to let the user maintain control of their own data. From a technical point of view, the accountability principle of the GDPR highlights the role of the data controller required to adopt technical and organizational measures to guarantee an adequate level of security, taking into account the risks, the state-of-the-art, the operational costs, the nature, the object, the framework and the treatment aims. Furthermore, the normative framework where data are managed should always consider the 1964 Declaration of Helsinki, as it happens with all health-related data aimed at scientific research.

4.1. Roles

When an SaaS solution is used, two entities are involved in data treatment, and both of them should be appointed a role within the treatment. According to Article 4 of the GDPR, when an organization uses the service offered by SaaS for its own aims, defining the purposes and means of the processing, this organization should be the data controller, whereas the service provider, when not directly entering within the merit of the treatment, is the data processor.

According to Article 28 of the GDPR, it is then required that the data processor has an explicit contract with the data controller.

Finally, for cloud services, it is particularly important to know where data are physically located. In cases where servers are located within the European Union, as in the case of the Health360 platform, the GDPR is always valid, as it is valid for data related to European citizens even when treated outside EU territory.

4.2. Lawfulness and Aims

The legal basis on which to judge processing lawfulness largely depends on its aims, and on the use or provision of an SaaS application; it must rely on Article 6 and Article 9 of the GDPR. Health360 was mainly developed as a tool to support research and to eventually support diagnosis. When the platform is used by healthcare providers aimed at research, with data collected for care aims, such a processing must have a different aim with respect to the initial one, configuring as a further processing. Under the GDPR's Article 5, Article 89 and Article 9, it can be derived that it is possible to use data, collected for care, also for scientific research; however, it is still unclear whether such utilization is prefigured as different from the initial one. This doubt is clarified by the Privacy Code, Article 110, par.4, where, except for Research and Care Institutions (the Italian IRCCS), affirming that the request for consent for scientific research aims configures this use as a further use than the initial one.

To date, the platform is employed to collect data directly on the patient with their consent (as required, in Italy, by the Privacy Code and by deontological ethics) to process data also for research purposes, therefore their use is not configured as a "further use" from the initial one.

4.3. Data Minimization

In the Health360 application framework, where it is needed to collect a wide amount of data, without knowing, a priori, their effective necessity (e.g., after statistical analysis, it can be discovered that several features are not useful to predict the outcome, etc.), the data minimization principle is difficult to apply. However, it is still possible to apply it when considering the whole data processing life cycle, split into its parts, collection, access and storage time.

Therefore, under such premises, the second phase becomes particularly relevant, that is to say the limitation of data access to just the operators that effectively need to access identification data of each patient, managing roles and privileges and pseudonymization. Finally, storage time should be evaluated with respect to the time window effectively necessary to carry out any scientific research dealing with such data.

4.4. Technical and Organizational Measures

The GDPR Regulation Article 32 manages security aspects within personal data processing. With respect to previous regulations, minimal measures (at least within the Italian framework) are not provided anymore, but the responsibilities to adopt all technical and organizational measures are now the responsibility of the data controller, based on the accountability principle (Article 24 and beyond). However, member states are left with some maneuver margins, especially in particular cases, such as those of genetic and health-related data in general.

It is often tricky to identify all the risks concerning data processing; among the most useful tools in this respect are those by ENISA, the European Agency for Cybersecurity, and in particular a risk self-assessment that an event, potentially harmful for treatment security, can occur, and the impact it could have on freedom and rights of the interested person, if data confidentiality, integrity and availability are compromised. The measures suggested by this tool are based on those defined for ISO 27,001 certification, and to this extent the impact assessment, requested by the GDPR through Article 35, is pivotal (see Section 4.5):

- Data confidentiality: Physical environment where servers are located should be made safe in terms of user access through authorization and tracking systems. Communication should also be equipped with Intrusion Detection/Prevention Systems (IDS/IPS) for monitoring network connections, detecting anomalous traffic and acting to notify or limit it. Communication could also be cyphered, and stored data, too.
- Pseudonymization: Health360 implements pseudonymization as a technique to join data to each other, especially when collected in the different software modules within the back-end, where personal and identification data are stored within the core module. Disjoint treatment, as required by the regulations, is embedded within the distributed back-end principles, enabled by the employment of the container architecture, simplifying software management of the different modules within different machines.
- Multi-factor authentication: Within Health360, this procedure is implemented using an authentication framework, Keycloack, widely used and supported by RedHat. The usage of a framework enables greater scalability with respect to other authentication solutions. An OTP generator is also used, employing commercial solutions (Authy, Google Authenticator, Free OTP, etc.) simply requiring an initial configuration (e.g., through a QR code generated by the platform) with two software systems synchronizing and generating a password depending on a time window.
- Roles- and attribute-based authorization (see Figure 3): The Health360 platform aims to collect a great amount of genetic data to improve results obtained by the data mining and Machine Learning algorithms, therefore the access to the platform is limited to only authorized personnel and to the data they have to access. Within the platform, several mechanisms have been developed that allow access to patients for healthcare institutions and, within the institution, depending on the role, keeping active the possibility to execute elaboration algorithms on the whole dataset. Identification information for the patient between different centers is visible just through explicit authorization mechanisms, based on the patient's authorization or in case of necessity and after the registration of the operator allowing the access, with the motivation reported.
- Data integrity and availability: Redundancy measures have been implemented within Health360. At first, all modifications performed on data do not modify the existing data, but they add (through an "append") the new data, recording the operator identifier and the motivation of the editing procedure. Second, caching technique was applied. As such, the user accesses to the remote front-end of the application, in turn accessing to the back-end, potentially located on different servers, to retrieve data or execute data elaboration. Health360 implements two levels of data caching (Figure 4), the first of which is on the user browser, using the IndexedDb technology, commonly implemented in any browser nowadays [23], allowing for locally saving data inserted in a form before sending such information to a server, in order to retrieve them if something goes wrong. More specifically, the IndexedDb caches all the data among work sessions, with the main aim for this being the prevention of accidental data breaks. A second level of caching is implemented on the front-end, at the graphical user interface level, to save the information retrieved from the back-end, making them available in case of connection absence with the latter, through Redis (classified as associative database). At the back-end level, a MongoDB is available, to manage all the data with the highest level of flexibility, seeing as the database is schemeless.

Figure 3. Role-based access control outlook: a user is assigned a role, previously charged with privileges.

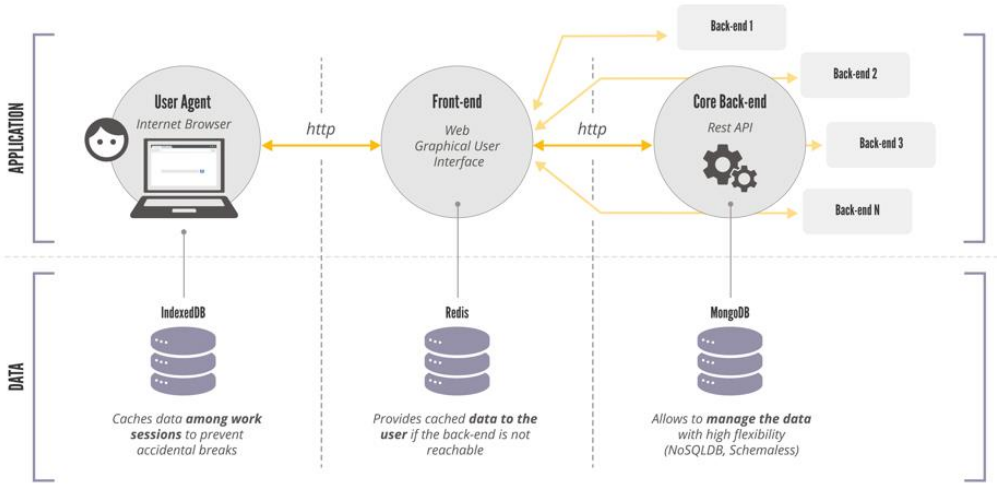

Figure 4. The two caching data levels implemented within Health360.

4.5. Impact Assessment

Overall, the data protection impact assessment (DPIA) should be completed in case of high risks highlighted during the risk assessment procedure. However, according to the European board, the DPIA must be filled in nine cases (extended to twelve in case of the Italian Privacy Authority), as mentioned below: (1) evaluation or assignment of a score, including profiling and forecasting, in particular in consideration of "aspects concerning professional performance, economic situation, health, personal preferences or interests, reliability or behavior, location or movement of the interested party"; (2) automated decision-making process that has legal effect or similarly significantly affects people; (3) systematic monitoring of the interested parties; (4) sensitive data or data of a highly personal nature; (5) large-scale data processing; (6) creation of matches or combination of datasets; (7) data relating to vulnerable interested parties; (8) innovative use or application of new technological or organizational solutions; (9) when the processing itself "prevents data subjects from exercising a right or making use of a service or contract".

In the specific case of the Health360 platform, the collection of health-related data is included within those criteria, therefore the DPIA must be performed, thus identifying not only the risks concerning data, but also the impact on the freedom and rights of the interested party.

The choice concerning the measures to be implemented should be the natural consequence of this process, with the aim to mitigate the risk level. In case such measures are not sufficient to decrease the risk level, or adequate measures could not be implemented, the Supervisory Authority should be contacted for authorization to conduct the treatment.

4.6. Privacy and Cookie Policy

The SaaS service provider should provide all the necessary information needed by the interested user to understand how and why their own data are treated, if from third parties, or outside the European Community, whether automated profiling mechanisms exist, and so forth. The GDPR's Article 13 and 14 fully specify this point (and Article 12 specifies how that information must be provided). Data collected are not only explicit ones, but also implicit ones, such as the IP address, the device used to navigate the web, and so forth, making a Privacy Policy always necessary. Cookies are also needed to improve

the user experience but also to collect data useful to profile the user. According to the European normative, profiling cookies are explicitly asked to the user (through an "opt-in") that should be flagged by the user to be compliant with the European regulation.

4.7. Non-Personal Data Treatment

Non-personal data are also particularly important in todays' society, given their potential application in several domains, especially commercial ones, therefore they are also required to adhere to specific rules. The rules on non-personal data are particularly critical when dealing with cloud systems, therefore SaaS applications, by professional organizations (B2B). Such rules aim to solve issues concerning the development of a digital economy within the European economic area, particularly concerning vendor lock-in and data localization required by some national rules or laws within the private sector, including certifications which are valid for just one member state or similar cases. Data lock-in occurs when inserted data within a cloud cannot be imported to another cloud system as featuring a proprietary format, without the possibility to be converted to another open format.

Furthermore, the European Commission encourages the elaboration of codes of conduct to foster systems' interoperability, to foresee minimal information obligations, to enhance the adoption of certification systems to compare products and services for data treatment, as demonstrated by the existence of a European Regulation [24].

Under those premises, Health360 was conceived in those terms, with the platform able to export data in a common, structured format, such as "comma separated values" (.csv) or other open formats.

5. Conclusions

Nowadays, the attention paid to security and privacy issues when dealing with software platforms is particularly critical in light of the key importance of data access and use in actual society, both for research purposes and for commercial use. In this paper, a specific use case, represented by the Health360 platform for data collection developed to acquire data concerning neuromuscular diseases, but not necessarily limited to them, was presented, together with an outline of the main measures implemented and some citations about the current rules, particularly dealing with the European normative. Health360 could be a useful alternative, filling in an important gap with respect to actual state-of-the-art of electronic health records, providing clinicians from small clinical centers or researchers within research projects with a tool featuring modularity, accessibility, ease of use, safety and data protection.

Given the unprecedented attention paid to data in any aspects of daily life, and the rising challenges associated with data breaches and leaks, this sector will probably remain at the forefront of ICT-related research and associated legislation in the years to come. For this reason, and for the growing threats represented by the issues of privacy, data safety, security, especially when dealing with data produced by smart, connected tools, as well as by Artificial Intelligence algorithms, future tools should tackle such issues in a systematic, serious way. This is particularly true also when considering the role Decision Support Systems are starting to have in the medical world. Therefore, great attention should be paid to make best use of instruments developed to date, and continuously updating their countermeasures against intrusions and data privacy points of failure, to avoid serious issues, putting even the life or the safety of the patient community under threat. When properly managed, this can lead to a promising future, where technology is key to reach new milestones, but at the same time protecting the rights and healthcare of human beings.

Author Contributions: Conceptualization, R.C. and F.S.; methodology, R.C., F.S., A.T. and A.P.P.; investigation, R.C.; writing—original draft preparation, A.T.; writing—review and editing, R.C., F.S. and A.T.; supervision, R.C., F.S. and A.P.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research project is funded by Tuscany Region, Bando Salute 2018 (InGene 2.0 project).

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Pediatric Ethics Committee of the Tuscany Region (protocol code 155/2020, date of approval: 3 July 2020).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pramanik, P.K.D.; Pal, S.; Mukhopadhyay, M. Healthcare big data: A comprehensive overview. In *Research Anthology on Big Data Analytics, Architectures, and Applications*; IGI Global: Hershey, PA, USA, 2022; pp. 119–147.
2. Sofia Jonathan, G. Information Science in the Analytics of Healthcare Data. In *Integrating AI in IoT Analytics on the Cloud for Healthcare Applications*; IGI Global: Hershey, PA, USA, 2022; pp. 219–237.
3. Hong, P.; Herigon, J.C.; Uptegraft, C.; Samuel, B.; Brown, D.L.; Bickel, J.; Hron, J.D. Use of clinical data to augment healthcare worker contact tracing during the COVID-19 pandemic. *J. Am. Med. Inform. Assoc.* **2022**, *29*, 142–148. [CrossRef] [PubMed]
4. Lodha, C.; Dhingra, K.; Mondal, R.; Goyal, S. Smart Healthcare with Fitness Application. In *Smart Intelligent Computing and Applications*; Springer: Singapore, 2022; pp. 403–409.
5. Imamalieva, D. Recent Challenges of Big Data Application in Healthcare System. In Proceedings of the International Conference on Multidimensional Research and Innovative Technological Analyses, Online, 2022; pp. 121–124.
6. Raj, R.; Daneshgar, F.; Borhan, N. Evaluating Challenges in Using Big Data in Healthcare. In Proceedings of the Sixth International Congress on Information and Communication Technology, London, UK, 25–26 February 2021; Springer: Singapore, 2022; pp. 59–69.
7. Nakić, M.; Miklošić, I. Beyond Pen and Paper: Reimagining Assessment of Personal Relationships and Quality of Life Using Digital Technologies. In *Quantifying Quality of Life*; Springer: Cham, Switzerland, 2022; pp. 355–369.
8. Mascheroni, A.; Choe, E.K.; Luo, Y.; Marazza, M.; Ferlito, C.; Caverzasio, S.; Mezzanotte, F.; Kaelin-Lang, A.; Faraci, F.; Puiatti, A.; et al. The SleepFit Tablet Application for Home-Based Clinical Data Collection in Parkinson Disease: User-Centric Development and Usability Study. *JMIR Mhealth Uhealth* **2021**, *9*, e16304. [CrossRef] [PubMed]
9. Holland, C.; Stuber, M.; Mellon, M. Integrating an Innovative, Cost-Effective Electronic Documentation System for Undergraduate Nursing Students. *CIN Comput. Inform. Nurs.* **2021**, *39*, 736–740. [CrossRef] [PubMed]
10. Conte, R.; Sansone, F.; Tonacci, A.; Roccella, S.; Spezzaneve, A.; Rateni, G.; Tesconi, M.; Calderisi, M.; Fantacci, M.E.; Astrea, G.; et al. InGene: A multimodal approach to the genotype-phenotype association in neuromuscular diseases. In Proceedings of the 2018 IEEE 8th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), Berlin, Germany, 2–5 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–4.
11. Brito, G.; Valente, M.T. REST vs. GraphQL: A controlled experiment. In Proceedings of the 2020 IEEE international conference on software architecture (ICSA), Salvador, Brazil, 16–20 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 81–91.
12. Chaudhary, K.; Gupta, M. Analyzing IPL dataset with MongoDB. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 10–11 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 212–216.
13. Kuflewski, K.; Dzieńkowski, M. Symfony and Laravel–A comparative analysis of PHP programming frameworks. *J. Comput. Sci. Inst.* **2021**, *21*, 367–372. [CrossRef]
14. Adam, S.I.; Andolo, S. A new PHP web application development framework based on MVC architectural pattern and ajax technology. In Proceedings of the 2019 1st International Conference on Cybernetics and Intelligent System (ICORIS), Bali, Indonesia, 22–23 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 45–50.
15. Lim, K.R.Q.; Nguyen, Q.; Yokota, T. Genotype–Phenotype Correlations in Duchenne and Becker Muscular Dystrophy Patients from the Canadian Neuromuscular Disease Registry. *J. Pers. Med.* **2020**, *10*, 241. [CrossRef] [PubMed]
16. Conte, R.; Tonacci, A.; Sansone, F.; Diodato, G.; Scudellari, M.C.; Grande, A.; Pala, A.P.; Astrea, G.; Frosini, S.; Santorelli, F.M. PhysioTest: A dedicated module to collect data from physiotherapy assessments in neuromuscular diseases. In Proceedings of the International Conference on Neuro Rehabilitation, Pisa, Italy, 16–20 October 2018; Springer: Cham, Switzerland, 2018; pp. 805–809.
17. Conte, R.; Calderisi, M.; Giorgolo, F.; Ceppa, I.; Astrea, G.; Rubegni, A.; Frosini, S.; Bertocci, G.; Santorelli, F.M.; Tonacci, A.; et al. NeuroExam: A tool for neurological examination in neuromuscular diseases. In Proceedings of the 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), Ancona, Italy, 19–21 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 5–10.
18. Marfisi, D.; Fantacci, M.E.; Astrea, G.; Santorelli, F.M.; Conte, R.; Tonacci, A.; Sansone, F. MRIndex: A tool for evaluating muscle involvement in neuromuscular diseases from MRI images. In Proceedings of the 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), Ancona, Italy, 19–21 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 287–290.
19. Calderisi, M.; Ceppa, I.; Cassandrini, D.; Trovato, R.; Bertocci, G.; Tonacci, A.; Astrea, G.; Conte, R.; Santorelli, F.M. A Novel Approach to Gene Analysis: Gene Panels and Cluster Definition to Assist Genotyping Patients with Congenital Myopathies. In *Healthinf*; SCITEPRESS: Setúbal, Portugal, 2019; pp. 345–352.

20. *EN 301 549 V2.1.2 (2018-08)*; Accessibility Requirements for ICT Products and Services. European Telecommunications Standards Institute: Sophia Antipolis, France, 2018. Available online: https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf (accessed on 15 June 2022).
21. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies (Text with EEA Relevance). 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102 (accessed on 15 June 2022).
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed on 15 June 2022).
23. W3C. Indexed Database API 2.0. W3C Recommendation. 30 January 2018. Available online: https://www.w3.org/TR/IndexedDB-2/ (accessed on 15 June 2022).
24. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Text with EEA Relevance). 2018. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807 (accessed on 15 June 2022).