REPUBLIC OF ESTONIA
GOVERNMENT OFFICE

REPUBLIC OF ESTONIA
MINISTRY OF SOCIAL AFFAIRS

Study “Impact analysis of the management of validation of third party e-health applications and a study on interfacing them with the health information system”

Public procurement reference No.: 181853

Final report

Tallinn Science Park Tehnopol

European Connected Health Alliance

European Union
European Social Fund

Investing
in your future

The study was carried out at the Government Office’s request and was funded from measure no. 12.2 “Development of quality of policy-making” of priority axis no. 12 “Administrative Capacity” of the Cohesion Fund’s operational programme 2014-2020. The initiator and partner of this project is the Ministry of Social Affairs.

Table of Contents

Summary

The aim of this document is to summarize the analysis of legal and technical alternatives for interfacing applications with the health information system. The document is based on the report compiled within the study “Impact analysis of the management of validation of third party e-health applications and a study on interfacing them with the health information system”. The incentive behind the analysis is a strategic expectation for wider implementation of remote services in communication between Estonian health service providers and people. IT companies’ expectations of and issues with interfacing with the health information system were studied during the analysis. The answers to these challenges were sought by an analysis group from international experience, which was combined with the vision of Estonian e-health specialists. As a reference of international experience, around a dozen projects with ambitions similar to the Estonian health information system were selected, six of which were selected in turn for detailed interviews. Insights into legal and technical solutions that are used in connecting third parties to public medical data integration network were collected during interviews. Although the international examples studied introduced many necessary ideas for the structure of a connectivity solution, a specific holistic solution that would cover Estonia’s needs could not be found.

One of the main conclusions of the analysis is that there is no need to change the health information system regulations currently in force to meet the needs of IT companies. The problems are rather of an economic, organisational and technical nature, or arise from inadequate management of complexity. Based on the previous conclusion, the study group has made initial, short-term recommendations: to reinforce service quality and service-orientation in the administrative organisation of the health information system; and to execute a technical solution for issuing medical data upon the request of a data subject.

Designations and abbreviations

CHWIF	- Estonian Centre for Health and Welfare Information Systems
DPI	- Estonian Data Protection Inspectorate
DSP	- digital service provider
EHIS	- Estonian Health Information System
EU	- European Union
HCP	- health care provider
HIF	- Estonian Health Insurance Fund
HIS	- Health Information System
HSOA	- Health Services Organisation Act
ISA	- Information System Authority
ISKE	- system of security measures for information systems
IT	- information technology
MoSA	- Ministry of Social Affairs
PDPA	- Personal Data Protection Act

1. Cases, user stories

1.1. Types of user stories as per examples and their dimensions

User story cases are presented from a person's point of view (not that of the HCP or state/official). At the same time, services and solutions being created offer both doctors and all other health care providers (hereinafter 'HCP') opportunities and open up a new market for private service providers (e.g. digital service providers, hereinafter 'DSP').

Different dimensions (all connected and combinable) can be highlighted in the examples of all of the featured user stories:

- **Organisational**
- **Commercial, i.e. business and funding model**
- **Technical and architectural**
- **Security and privacy**
- **Legal solution in terms of HSOA and ICT**
- **Health care policy, political initiation**

1.2 First case: issuing HIS data

A person wants an electronic statement of all data collected in HIS concerning themselves (images, films, dynamics of lab analyses, diagnoses, medications, etc.) for the purpose of seeking a second opinion in e.g. Finland or as part of a self-funded appointment (chiropractor, orthopaedist, neurologist, gynaecologist, traditional Chinese medicine practitioner, etc.).

- An electronic format compliant with international standards (xml, pdf, dicom, etc.) is required.
- HIS offers a respective service for extracting data in the Patient Portal (various formats; extent and confidence limit may be differently priced).
- The HIS Patient Portal notifies a person of risks related to further use of data and asks for confirmation that the information has been read and acknowledged.
- The Patient Portal may also offer a combined service, where a person gives a private service provider informed authorisation, who then has authorised access to the HIS archive for requesting information.

1.2.1. Legal view

The Personal Data Protection Act **provides a person's right to obtain data concerning them**[1].

Despite the fact that the Act enables the **data to be issued in the manner requested by the data subject**[2], there is no technical and sustainable solution for issuing data electronically at present, which is why this problem is mostly solved on paper. How to issue data electronically in the future is described in this report's technical and architectural view.

People decide for themselves how they store/process their data, although professional advice is always appropriate.

Should **a person wish to seek a second opinion from another health care provider** on their diagnosis or treatment decision **based on their data**, it is enough if they turn to another HCP. This is seen as an application for receiving health care, where a person physically or electronically (e.g. using a personal account) provides their data to another health care provider.

If data is sent electronically, this is considered a **telemedicine service**, where another HCP takes a position on a medical issue based on the information obtained without meeting the patient. Currently the problems arising in providing telemedicine services are more technical in nature, as not all data can be sent digitally at present. There is no need to amend legislation to solve this situation.

Processing (including issuing from HIS) a person's medical data **at their request** is based on their agreement – data are sent straight from HIS to the service provider (DSP) the person chooses. There are a number of conditions[3] an agreement has to meet, but the most important are that the agreement for using such a service is based on free will, only relevant data are used as part of it and that the data are processed securely.

Processing sensitive personal data as part of such services requires it to be registered with the **Data Protection Inspectorate** (PDPA chapter 5), and should the data be sent to a third country (i.e. outside of the EU), appropriate permission from the Inspectorate is also required (PDPA §18).

1.2.2. Organisational and commercial view

Elementary service in HIS Patient Portal. It would be easiest to offer people the chance to download data to their personal computer as a choice between multiple formats. This could be a paid service whose price was not very high. All technical and legal requirements exist for the creation of this service. The service could later be linked to a patient's personal account and its administration and the service as a whole could be outsourced, if such a practice existed.

[1] PDPA §19 section 1

[2] PDPA §19 section 2

[3] PDPA §12

1.2.3. Technical, architectural and security

This is a one-way service where responsibility in the further use of data lies entirely with the person and there are no requirements for further data processing. Only logging in to HIS and accessing services are subject to requirements. An overview of the interfacing activities of digital services that process data with the data subject's consent is provided in section 4. Interfacing activities of digital services and the principles of validating the security of digital services in section 3. Certification of a digital service.

1.2.4. Health care policy, political view

Creates a presumption that people take responsibility for their own health. The service includes a strong awareness-raising component. When issuing data, a person should be notified of risks and be provided with recommendations on safe data processing. The service creates a foundation for private services to enter the digital health market.

1.3. Second case: new services for HIS data

A person/doctor wishes to use services based on the data collected in HIS by themselves or other HCPs (with different levels of difficulty or complexity):

- **reminders** – next vaccination (for themselves or their children), next date on which to provide a sample for analysis to monitor a chronic illness, next appointment, participation in screening, etc.
- **visual excerpts (charts, images, etc.) over time** – e.g. blood sugar, blood pressure, PSA markers in blood, various markers in blood and other bodily fluids or tests (including MRT).
- **monitoring services** – for monitoring various diagnoses or for after-care (e.g. heart attack, stroke). The treatment guide includes the frequency and values of monitoring and benchmarks.

Despite the fact that the spectrum of services provided in the described case is broad, it is characterised by the fact that the existing data are used for providing services and a new appointment is not required before a service is provided.

In simpler cases the service assists people who care about their health.

In general, similar services form part of the HCP quality system, enabling doctors to easily visualise large amounts of data that to that point have remained separate pieces of data on separate pieces of paper. Such services raise the quality and effectiveness of work, making data collected over time usable. The services are necessary for doctors to monitor patients' long-term data and health dynamics, especially in the case of chronically ill and elderly patients. When doctors and nurses are obliged to look at collected data in their work, it requires smart, fast and convenient technical solutions based on current data, saving time for doctors and nurses.

1.3.1. Legal view

Since the service can be designed for both people (a person places an order and pays for it themselves) and health care providers (HCP (Health Insurance Fund) places an order and pays for it), the cases need to be considered separately.

When an **HCP orders/buys a service following a treatment plan**, the service is provided as part of health care and data processing takes place in accordance with the applicable law (HSOA, PDPA). There would be no need to amend legislation to solve this situation if service provision did not require changes in organisation of health care policy and hence adjustments to the system of service financing. Today the Health Insurance Fund does not finance such services (fully automatic decision support, digital treatment guide, etc.), although it could be considered for the sake of better health care provision. Current practice is limited to various IT solutions HCPs have outsourced at their own responsibility and integrated into their information systems, instead of using distributed data.

If a person buys the service themselves (e.g. for managing their health), it is sufficient for them to **grant consent (authorisation) to their chosen service provider (DSP)** to process their data. People are willing to pay for the service themselves, which helps more widely open up the market for services that support health management.

DSPs need authorised access to data. There is no technical capability for this currently – its prerequisite is a HIS service combined with the Patient Portal (as a service under a person's authority) or DSPs' access to the HIS data archive under the authority of either a person or an HCP. In the first case, a person authorises access to data and the system provides access to the data archive (a clumsy and not particularly sustainable solution, as it is one-way and the person has to repeatedly authorised access to the data). In the second case, an HCP entrusts a third party to offer a useful technological solution as part of their service – for instance Medipost (operational today) and Dermtest and other planned ideas. Such solutions could advance more quickly if the HIS/CHWIF service package included standardised services.

One major obstacle is rigid health care management, bottlenecked by HCPs' lack of motivation and ability to implement new technological solutions. Health care management methods do not promote innovation in, for example, service quality, assessment of treatment results and adding them to the list of services covered by the Health Insurance Fund (insurer). The patient as the policyholder has no means of affecting this list of services. The policyholder's ability to choose a service provider and services is infinitesimal – everything is regulated in contracts between HIF and HCP and the list of services/price list of HIF. The current health care management and pricing model has not promoted the greater introduction of technologies via the involvement of the private sector and patients. It has created a certain business model monopoly by the state. Services improving treatment results, quality and doctor's time could be the object of HIF's price list. Its alternative is paid services that keep appearing on our health care market, coming from both domestic and global markets. Their downside is the general polarisation of service availability, especially if the state and HIF still do not take steps to open up and regulate the market.

The service must be certified from both the technical and medical perspectives, besides reminders for patients. A medical statement of compliance is important in assuring future users of the service's quality, i.e. the medical information provided is reliable and comprehensible and the service is therefore capable of creating value. A technical statement of compliance is important for making sure that health care providers can use the service (e.g. it has to comply with standards, measuring devices must be calibrated and units of measurements must comply with requirements to make them comparable). In short, such services must follow the same safety requirements as HIS.

The service is universal and suitable for cross-border use if international data standards are followed.

1.3.2. Technical, architectural and security

In simpler cases this is a one-way service provided at a person's responsibility. In more complicated cases it is a service following the same rules as services provided by HCPs. The interfacing process of digital services processing data with the data subject's consent and security principles are further explored in the document's other sections (4. Interfacing activities of digital services and 3. Certification of a digital service). Since a data subject can process medical data using a random digital service, the recognition (certification) rate of the given service can only be recommended. Users should opt for digital services deemed safe from the perspective of health or data protection.

1.3.3. Organisational and commercial view

A service solution depends greatly on **who pays for the service** and is thus mainly a health care policy-related issue. If the service is needed by a health care provider, it is paid for by the Health Insurance Fund; but if a person needs it, then it can be paid for by the person or the Health Insurance Fund, depending on the political decision.

The main problem with the current financing model is that the Health Insurance Fund does not sufficiently motivate prevention via its funding principles, nor does it buy treatment quality, which is why health care providers lack the motivation to provide and further develop the services described in this case. If we were to link the Health Insurance Fund's financing model with the obligation to electronically monitor the treatment guide, this would create a mechanism for the emergence (creation/implementation) of such services among health care providers.

In terms of opening up the market to third parties, it would make sense to consider the option of people paying for the service themselves or being able to use the Health Insurance Fund's finances for prevention and managing their health.

In the current health care management situation, such services could only be provided on the basis of people paying for themselves – a digital service provider gains authorised (person's consent) and certified (statement of compliance with requirements foreseen by an authorised institution) access to data and provides a person with paid services, such as:

- people subscribe to reminders
- people subscribe to services that monitor the dynamics of indicators of diabetes or other chronic illnesses
- people subscribe to reminders of the health indicators of their parents (who are elderly and being monitored) or from sensors that monitor them

1.3.4. Health care policy, political view

DSPs need authorised access to data. There is no technical capacity for this currently. The main obstacle is rigid health care management along with a business model monopoly. Opening up the market for such services will definitely have an impact on health care management as a whole, since not everyone can afford the service.

- **The service must be certified from both the technical and medical perspectives**, besides reminders for patients.

- The service is universal and suitable for **cross-border use** if international data standards are followed.

Health care policy is an important trigger mechanism for the services in this case group. It has been proven that the prevention and monitoring of chronic illnesses have an effect on health and are cheaper (CVD, diabetes, etc.). Also, monitoring and checking risk factors along with keeping an eye on health behaviour. It is becoming increasingly popular to financially motivate people to take responsibility for their health (to discourage a doctors-will-fix-me mindset). For example, dividing up health insurance money between a solidarity fund and a private account where people themselves select their service providers and which prevention packages they participate in. People are also motivated to look after their health via higher/lower health contributions – the procedure can be automated using digital devices and monitoring and thus the health contribution can be lowered (or higher contributions be taken from others). It is also possible to automate preventive screenings in the primary care/general practitioner systems according to people's health profiles. Personal health profiles can be used to systematically provide people with personal preventive/promotional programmes, etc. All of this can be influenced via state policy, using automated solutions for providing health care through the HIF price list and models of financing:

a. Along with the planned general practice centres, electronic automatic programmes corresponding to a personal health profile are also introduced in interaction with a quality monitoring system within a general practitioner's capitation (from HIF's budget or EU contributions).

b. Launch an innovation foundation in HCPs in cooperation with HIF and the private sector for developing such services. The foundation should include contributions from HIF, the EU and the private sector (private investors), which would speed up the integration of new technological solutions. Later services could be bought by people or HIF and be suitable for the international market as well.

1.4. Third case: people introducing additional data to HIS

A person wishes to electronically (not on paper as a diary) send a doctor information on data they have collected (which the specialist or general practitioner asked them to note down) – blood pressure indicators, number of steps taken or any activity, food diary, frequency of going to the bathroom, insulin administration diary, etc. (Plenty have been issued in print.) Similar data entered by patients could be device-based or manually entered following the approved standard:

- Technical solution for the necessary service of the HIS Patient Portal for manual or device-based data input;

- HIS/ISA together offer a certified service for registering products along with standardised calibration procedures;

- CHWIF/ISA offers a service for interfacing certification along with consultations on completing the procedures;

- People are offered consultations for choosing (from some sort of depositary) technically certified applications (paid applications and devices) and paid approved services (e.g. by HCPs in a medical sense).

A large portion of the listed services can be offered by authorised private service providers, not necessarily ISA or CHWIF. The state needs to define the requirements and hold a public procurement to outsource an operator service. In the longer term the listed services can be linked to other services and developments in a wider sense:

- Can be connected to a personal medical data account;
- Data can be integrated with HCP's data on doctors' desktops;
- The service can be offered on the private market;
- The same service can also be bought by people for preventative purposes.

1.4.1. Technical, architectural and security

This opens up a private service market where the state needs to regulate services, as these are also health services and in some cases it may be necessary to use the data collected by the services in the health care system (HIS). In such a case the requirements for two-way data travel are as high as those followed by HIS. If the services remain on the private market, users must be notified before issuing data, but users personally assume the risks related to data safety and quality. Notifying must be in a form usable for subsequent reference.

1.4.2. Legal view

If a doctor tasks their patient with collecting data or presenting data to their treating physician **as a art of health care**, the data are processed following the laws currently in force (HSOA, PDPA). There is currently no direct obligation to collect data in a certain way, besides a health care provider's duty to document data[4].

Although documentation began with drawing up, maintaining and issuing paper records, the health information system was created to better fulfil this duty, with the purpose of documenting facts concerning people's health with enough precision, detail and frequency and where data processing and retention are regulated in various legal acts.

Although the duty to document falls to the doctor and patients have the right to request data, this does not mean that doctors, while providing health care, cannot ask patients to keep an eye on their condition and note the necessary markers. Establishing the requirement that data are always collected and provided electronically, taking into account above all that digital data processing increases the availability of data, should probably be considered; plus it is easier to ensure their integrity and confidentiality, since data acquisition on the basis of database basic data provides better (up-to-date) results and electronic security measures enable you to leave a trace if a document or data have been viewed (who, when and to what extent the data were accessed).

[4] The duty to document is a contractual obligation of a health care provider, laid down as follows in the Law of Obligations Act §769: "A provider of health care services shall document the provision of health care services to each patient pursuant to requirements and shall preserve the corresponding documents. The patient has the right to examine these documents and to obtain copies thereof at his or her own expense, unless otherwise provided by law."

Since we are dealing with a **therapeutic relationship** here, it should be checked whether HIS has the required data content. If data input to HIS of this kind is regulated, there is no need to amend legislation to solve the situation. If not, **the new data content needs to be added to the data content of a regulation on data provided via HIS.**

Hence, before opening up a new service, we need to define the data content, standard and object module, for instance, in the Patient Portal along with integration with information systems of HCPs, which means that the problem is technical/organisational.

The same data and technical solution can also be used to **provide data and monitor health profile over time on a person's own initiative.** People could buy services based on these data for prevention purposes and later, if an illness occurs, monitor its dynamics with a doctor (in a therapeutic relationship). Use of paid services for the purpose of independent prevention of illnesses takes place on a person's own initiative and with their consent (authorising DSPs to process data). If an illness occurs and the data collected for preventive purposes is later analysed with a doctor, this initiates the legal scheme described above (data processing according to law – HSOA and PDPA).

There is no need to amend legislation to solve this situation.

In an organisational sense, what matters is whether the case is solved following scenario B or scenario D (see the scenarios in section 2). If CHWIF starts providing everything itself[5] (i.e. scenario D), it would need a marketing and sales department, a certification department and perhaps even more. If these service are outsourced[6] (scenario B), i.e. private-sector entities are authorised to provide them, laws should be amended to allow some acknowledgement, certification and authorisation roles to be handed over from the state to the private sector.

In an organisational sense, it depends whether a competent state institution starts offering all services related to certification, standardisation, etc. (also designating a monitoring-competent state institution or inspectorate) or whether a competent authority (a state institution) is laid down in law to carry out (coordinate) certain tasks and the service is provided by a service provider on the trusted list.

If paid services are introduced at the state level, the corresponding provisions must also be laid down in legislation (State Fees Act).

1.4.3. Organisational and commercial view

Depends on who provides the service (similar to the previous one).

The service solution depends on who pays for the service (thus making it a health care policy-related question):

a. if HCP needs the service, then HIF

b. if a person needs the service, then either HIF or the person

[5] E.g. CHWIF itself certifies applications, allows access to data archives or standardises.

[6] E.g. CHWIF does not certify applications, allow access to data archives or standardise itself. All of this can be outsourced, but operators need to follow requirements and sign a contract. Just as the electronic health record maintenance service used to be provided by a foundation.

Today the problem lies in the fact that HIF does not purchase treatment quality, which is why the HCPs have no incentive to develop such a service. If HIF were to link the obligation to monitor treatment guides using electronic services with funding, it would create an incentive to create such services within HCPs.

Business-wise it would be better if private funds were also included in the business model through people – people could either use their own money (in addition to HIF's) or, if covered by insurance, use HIF funds as they prefer.

With current health care management these services could only be provided if people were willing to pay for them – a private service provider gains authorised and certified access to data and offers people paid services, such as:

- people subscribe to reminders
- people subscribe to services that monitor the dynamics of indicators of diabetes or other chronic illnesses;
- people subscribe to reminders of the health indicators of their parents (who are elderly and being monitored) or from sensors that monitor them

1.4.4. Health care policy, political view

In a political sense the principle should be that data are provided and transmitted electronically throughout the health care system and paper documents are an exception to be used in certain cases only. Patients are provided with a standardised object module in the Patient Portal with which they can interface their devices and transmit data to doctors and their own account for preventive purposes. See case 2 in section 1.3.

1.5. Fourth case: personal medical data bank

A person wishes to **collect of all their patient data in a single account: *My medical data bank***, whereas their data is scattered between HIF, various devices (blood pressure, steps taken, calories, etc.) they use, the genome centre (genetic data and tests), separate service providers (e.g. Synlab) from whom they have purchased a laboratory examination of their general health situation, healthcare consultancy information from the same or other service providers (e.g. Synlab, Dermtest), etc.

The person is **willing to pay a monthly subscription** for account management (similar to a bank account) to safely store the data if it is guaranteed that they will be retained despite the success of third-party service providers (bankruptcy, etc.).

- Need to define the criteria for the operator of a personal account (the service can be provided by both HIS/CHWIF or a private service provider). As a private service, it is recommended to outsource an international operator service and issue it with a state guarantee.
- Need for a data standard, which can be based on international and HIS standards and experience (possible to utilise the experience of banks and the idea of a data repository).
- Can be linked to e-residency to solve the authorisation/authentication problem.

- Access to data is authorised by a person.

This vision is a combination of an international dimension and previous cases for the involvement of the private sector to a great extent and to provide services authorised by the person. It is a suitable addition to Estonia’s e-state service portfolio in the EU context – see the global scenario.

1.5.1. Technical, architectural and security

Medical data banks may have different solutions from the point of view of security certificates.

- Data are processed based on an agreement between a user and a DSP. Different digital services can allow different privacy or health security conditions. The user themselves chooses the method for monitoring whether these conditions have been fulfilled. EHIS data can be issued for such digital services with the data subject's consent.

- The data processing has been deemed to correspond to the level required to add EHIS data (S2T3). This system would allow EHIS data to be added and reviewed at health care providers’ responsibility (if there is a therapeutic relationship) and shared via EHIS with other market players if EHIS adopts interoperability standards for data added by a person.

1.5.2. Legal view

The legal approach is similar to the previous case, relying on a person’s informed authorisation. People need to pay for the service, as it stores both data collected for preventive purposes and from HIS. The success of its realisation depends on an organisational/commercial solution, which will need to be described in greater detail should the state wish to use such a solution. See the commercial view. Establishing the database would only require a legal basis if *My medical data bank* were to become a national database. If not, it would be a service provided by a private body, where the service provider should be accredited by a competent authority and the service’s compliance with legal acts and standards checked.

1.5.3. Organisational and commercial view

The commercial view is similar to subsection 1, where people retrieve data at their informed responsibility and pay for their health accounts themselves to ensure data retention. But it is important to note two things in terms of the operator service:

a. The data from this account will at some point become necessary for HCP, i.e. HIS and health account standards must be compatible both ways (otherwise there will be duplication).

b. It is important for data retention and other requirements for the operator that there is an obligation to guarantee data retention and that the state provides supervision (similar to outsourcing the hosting service), but the state does not have to make a 100% financial contribution. It should be an international commercial project covered by a state guarantee.

1.5.4. Health care policy, political view

The decision to create a personal health account is a national international initiative that can be linked to e-residency. Its prerequisites are better compatibility of HIS standards with international standards, the availability of a data repository and technical access to it and two-way compatibility of data moving from and, if necessary, back to HIS or from a personal account straight to HCP.

Such a project has the potential to become a new HIS with an international dimension and perhaps in 10 years our HCPs will also use people's personal accounts (that hold both medical data and data collected by people themselves) instead of HIS.

1.6. Fifth case: personal authorisation

A person wishes to grant additional authorisation or make declarations of will in the Patient Portal:

- Permission to view their time-critical data in an emergency;
- Permission to access their data with the purpose of providing a specific service by DSPs or other cases, such as when calling the general practitioner hotline (1220). Authentication over the phone requires a technical solution;
- Permission to anonymously use their data in research, provided they are notified where the data was used;
- Permission to be invited to participate in clinical trials for expanding treatment options for chronic illnesses, clinical trials for rare illnesses, testing new medications for certain diagnoses, etc.;
- Permission to anonymously use their data in big data analysis;
- Permission to use their data to be invited to a screening.

Need for technical capability (HIS services) and developments in the Patient Portal along with notifications to people, HCPs and entrepreneurs. Entrepreneurs shall have special criteria and requirements for accessing data after they have been granted authorisation by the person.

To open up the market for such a service, the prerequisite is to create a service for private service providers to access the HIS database.

1.6.1. Technical, architectural and security

To accept people's data (including declarations of will) we need:

1. Agreements on data's definition, coding and format and in other areas of interoperability. Interoperability agreements can be developed by any party in cooperation with the operator (CHWIF), who can guarantee sufficient quality.
2. A high-security digital service to collect, transmit and present data.

1.6.2. Legal view

§21 section 1 clause 1 of the Health Information System Statute stipulates that data subjects have the right to make declarations of will via HIS or to present them to authorised data controllers or processors to deny or allow access to their personal data. Thus the HIS statute could be clarified in terms of different declarations of will regulating access to personal data for clarity's sake, but there is no immediate need for this, as the statute does not regulate this issue in great detail.

One way to grant consent would be to **create a platform for patients' approval in the Patient Portal that a patient could use to grant and withdraw consent to process their personal data**.[7]

Consent[8] granted by a patient has to be willing, specific and clear, clarifying, among other things, the data for which processing permission is being granted; the purpose of data processing; the people to whom the data can be sent; the conditions for transferring data to third parties; and the person's rights in terms of the further processing of their personal data. The person must also be notified of the name of the data processor or their representative, their address and other contact information before consent is granted. If the personal data is processed by a data controller and a data processor, the person shall be notified of or given access to the names of the controller and processor or their representatives, their addresses and other contact details. It should also be taken into account that the person shall always have the right to withdraw their consent and the data processor has the obligation to prove the existence of consent.

There is no need to amend legislation, thus making it a question of service development and technical solution. And a question of payment. If private services are included as partners, this will create interest and those who will pay for the service.

1.6.3. Organisational and commercial view

The main obstacle right now is organisational/commercial in nature, i.e. who pays for it. If the market were opened up and the portal's technical solution for declarations of will were linked to issuing data with a person's consent as a paid service or to a health account, the same solution as mentioned in subchapter 1.3.3 could be used.

1.6.4. Health care policy, political view

It depends on the state as the owner of HIS as to whether they wish to open up the service market. Not all residents have the same purchasing power, which is why there is a need to consider compromises and assess balance between HIF funding, private investors, people's own contributions and, for instance, a combination of the funds of pharmaceutical companies and the EU.

[7] A similar scheme is under development in the context of the work ability reform in terms of sending people's medical data between the Unemployment Insurance Fund, the Social Insurance Board's information systems and HIS; see "Solution for IT and legal issues of medical data movement required for the implementation of the work ability reform"

[8] More specific requirements arise from PDPA

All in all, e-services create opportunities for people, health care providers and companies alike. The critical difference compared to the current situation arises when new cases emerge as per the decision of a data subject that are not currently regulated in HSOA, but in the PDPA's general provision.

The difference arises where people **willingly** take the risk and **willingly** buy low-security services or those without a guarantee. In this case they must have the right to withdraw from such a service and under certain conditions return their data to HIS or their personal account. 'Willingly' is emphasised because it is stipulated by the law and the person must be informed – such an obligation must be implemented in the Patient Portal and in procedures for creating a personal health account.

In all of the cases listed above, HSOA or PDPA allow the services to be provided if the patient grants consent to a DSP. Or if a DSP provides their service to a doctor (HCP) instead.

All cases require a technical and organisational solution.

In most cases, implementing acts need to be amended, either in terms of data content or outsourcing:

- Certification of DSPs;
- Certification of applications (in terms of devices) and the corresponding repository (disclosure of their list to people);
- Data standards and standardisation taking the international dimension into consideration as much as possible;
- Access procedures, managing access and authorisation and development of the corresponding services.

Health care policy-related choices and decisions need separate options and regulations connected to the emergence of new possibilities to implement health care policy:

- Connect people's health behaviour to the amount of health contributions;
- Connect general practitioners' quality system and remuneration with monitoring chronically ill people and their recovery/prolonging their healthy period;
- Create a new market and economic growth by outsourcing some of the services – certification of DSPs, conformity checks on interfacing, data repository management and creation of a paid DSP service market.
- Create mechanisms for integrating services with HIF – include e-services in the price list, how to motivate HCPs to use data analysis technologies;
  - Create an 'innovation foundation' together with HIF, the Connected Health cluster and the private sector (including private equity);
- Create a project of international interest:
  - A database-wide e-doctor along with recommendations as a prevention measure;

    - HEALTH ACCOUNT that is linked to e-residents to store personal medical data (including device-based data) with HIF-like data (XML, DICOM, HL7, etc.).

2. Scenarios

Upon designing the analysis scenarios, the study group of this study regarded the following dimensions of digital services:

- Party responsible for data processing
    - Health care provider’s responsibility
    - Data subject’s responsibility
    - Digital service provider’s responsibility
- Means of recognising data security and interoperability compliance
    - Recognition gained in a regulated manner
    - Without sufficient recognition
- Direction of data flow
    - Issuing data via digital services
    - Adding data via digital services

Reviewing the combinations of these dimensions, the following analysis scenarios were developed:

1. Adding and issuing data from EHIS at a health care professional’s responsibility.
2. Releasing data with the data subject's consent.
3. Adding and issuing data under a digital service licence.

	No regulated certificate	Regulated certificate
Health care provider’s responsibility	Use of EHIS data not allowed	Adding and issuing EHIS data at a health care professional’s responsibility
Data subject’s responsibility	Issuing EHIS data with the data subject's consent	Issuing EHIS data with the data subject's consent
Digital service provider’s responsibility	Use of EHIS data not allowed	Adding EHIS data under a digital service licence

2.1. Scenarios A, B, C, D and G

- A. BAU (Business as usual)
- B. Business-opened
- C. Citizen-commitment-oriented
- D. Domestic
- G. Global-oriented

A. BAU (business as usual) – maintain the current situation. HIS services are poorly integrated with health care management and the system of financing (e.g. there is no obligation to view electronic health records and remuneration for HIF services is not connected to adding or requesting information from electronic health records). Neither online data from HIS nor big data services are used for quality evaluation, decision support is not used and patients are not involved in collecting and electronically providing their own data. Electronic monitoring and follow-up treatment solutions are not used and private sector technologies have not been implemented in primary care-level prevention. The private sector does not have access to HIS data or the market for new services.

The given scenario is unlikely to create good conditions for opening new cases and user stories. The positive scenario foresees that the existing services become more stable, but a great deal of the technology's and market's potential remains modestly exploited. **It is highly likely that the only breakthrough will be the implementation of the first case, if they find funding.**

B. Business-opened – creating better conditions for the private sector's greater involvement in e-health services. Opportunities are sought depending on various aspects:

B1: how can HCPs be motivated to involve more new technologies and service providers to provide new solutions and solve their own services? The state finds economic means to involve private investors' money and increase health insurance funds to integrate new solutions with health care ('innovation foundations'). For instance, if the state decides that besides the agreed price and efficacy variables the **result of treatment and quality indicators** are also taken into consideration when treatment is funded and priced, then services built on collected data and digital services are of great use in connecting various treatment stages, including follow-up treatment, rehabilitation and survival. Also the examples in the Annex.

B2: outsourcing various roles and activities related to HIS administration and development, leaving the state (MoSA + CHWIF) with the role of a service market supervisor and regulator. For example, **moving the standardisation service into the private sector**, where the services of the state, HCPs and DSPs must follow the standards and these standards require a fee (similar to international standardisation organisations). Another similar certified third party could provide authorisation and procedures for accessing a data warehouse (or data repository) following the established and approved regulations.

B3: people or patients buy private services themselves using private services and can also reuse data collected in HIS (mainly global services).

This scenario creates suitable conditions for all scenarios, depending on whether any other factors are added that amplify a scenario – developments on the global market, technological development, people's attitudes and goodwill and other measures that promote business in Estonia (e.g. integrating start-ups with health care or other implicit factors).

C. Citizen commitment-oriented – people are given more freedom, possibilities and responsibilities to make decisions about their own health (which services they want to use, whom they buy services from, how many risks and responsibilities they are willing to take). In this scenario the possibilities can be implemented on the market for digital services and also integrated with health care management and its changes via new operational models.

C1: people use their HIS data to buy paid services and health services at their own responsibility (and with their own money, including insurance). People buy various technologies and services from both the local and global markets for managing risks, prevention and buying treatment services from insurance companies.

C2: the state decides to place, for instance, **1% of medical insurance funds at people's disposal** so they can buy any services from the private market (e.g. traditional Chinese medicine or services of global applications).

C3: the state decides that if people regularly reduce their health risks and engage in prevention, a 1% **lower health contribution** is collected from them – in such a case the person consistently collects and uploads their risk factor indicators to HIS (activity, blood parameters in terms of cholesterol, triglycerides, etc. according to the diagnosis or risks, also smoking and alcohol consumption, participation in general practitioner's prevention programmes and monitoring, etc.).

This scenario creates conditions for all cases, depending on whether any other means or barriers are added (health care policy, global market developments, living standards, etc.).

D: Domestic – the state increases its contribution and assumes a leading role to initiate innovation, develop services and manage them. **The state assumes responsibility for expanding services in cooperation with the private sector and for including people** and offers services on a wider scale to ensure their availability and even level.

D1: since this scenario means that state budget expenditure increases markedly and if the private sector is not authorised, **some services need to become paid services**, such as issuing data from the Patient Portal to people, issuing non-personalised data to science projects or third parties, compliance clearance for IT companies, technical consultation and legal counselling on interfacing and for people on creating their account and storing their data in paid services.

In this scenario, the first case will most likely be implemented, and if paid services serve as motivators, it will create conditions for other uses of data and service developments, as described in the fifth case of the user stories.

G: Global-oriented – the state promotes the development of global services by combining different scenarios. It is recommended to combine opening up the market to the private sector and attracting innovation and investors' money with an international project to introduce a project that may interest the global market, for example **creating personal health accounts for Estonian residents and e-residents with the aim of influencing the international standards market.** This opens up an opportunity for the private sector to offer standardisation and data warehousing operator services along with the respective authorisation. This scenario also gives people more options to use global services along with an increase in their own contribution (and freedoms).

In this scenario, the **first, second and third cases of user stories can be combined and conditions for completely new services introduced to the global market.** Integrating the scenario with the local health care market may in turn move in several directions. It may turn out that local HCPs start using the new opportunities related to services provided on the basis of personal account data, in turn creating conditions for moving from previous HIS solutions to a multifunctional service and data account (in this case the HIS database shall remain the system's data archive and its services gradually lose their relevance). Another possibility might be that local health care does not go along with global developments and over time the personal account solution becomes an international business, but local health care does not deem it necessary to realise its potential.

3. Certification and recommendation

Certification of services means proving their compliance with the requirements of a standard or another normative document by an independent third party. The volume of work related to certification depends on the complexity of the service to be certified, the size of an organisation and the number of sites. For a service to be certified, an audit is carried to check its compliance with a service standard or other normative documents. This includes assessment of documents, completed tests, etc., as a result of which a report is drawn up along with a description of any inconsistencies detected. Once the inconsistencies have been dealt with, the organisation's service is awarded with a certificate (for a certain amount of time, such as 2-3 years). During the certificate's period of validity the organisation's compliance with requirements is regularly checked via follow-up audits. Once issued, a certificate can be extended every 2-3 years (depending on how long it was issued for to begin with).

Certified services (service providers) are registered in a corresponding written or electronic list (register).

There is also a more traditional service recognition practice where there is no single standard or where a corresponding normative document or process has not yet been developed in the given field. Recognition may be verbal as well, for example acquaintances or opinion shapers may confirm the suitability of a product, smart person or service, which should be considered to be a more of a recommendation or advertisement.

Taking the above into consideration, we can divide the trust placed in services into two categories:

1. Regulated trust services or certification, where the services' compliance with a standard or another normative document is verified (by an independent party, e.g. a competent organisation);
2. Unregulated trust services or recommendations, where the principles of recognition are agreed upon at the company, community or personal level (opinion).

A trust service mechanism can be used in the field of digital health in several ways:

1. Recognition of a health service provider – awarding an operating licence
2. Recognition of a health care professional or a health consultant – awarding an operating licence
3. Digital recognition of the identity of an institution (identity of an x-road institution)
4. Digital identity recognition (ID card)
5. Recognition of the security of a digital service
6. Recognition of the interoperability of a digital service

3.1. Certification of a digital service

Certified digital services process medical data following the requirements provided by law and have been awarded with corresponding recognition or a certificate (i.e. have been added to a register). This does not automatically mean that a digital service processes data at the highest security level or heals its users of all diseases. Recognition simply shows its compliance with requirements, of which there may be many.

Certification of digital services is an important tool if services are to participate in the medical data exchange (processing) market.

1. A digital service security certificate for uploading medical data. When uploading data to the health information system, a high integrity requirement (ISKE T3) is implemented to ensure the data subject’s safety and the quality of the medical decision. High integrity links data and their sources in a way that can be irrefutably proven.
    a. In one case a digital service or device has been proven to correspond to the requirement of high integrity. Data collected by a digital service are considered true as set out in its terms of use.
    b. In another case a person is responsible for the correctness of their data. A health care professional or the person themselves prove the correctness of the data every time data are added.

2. A digital service security certificate for releasing medical data.
    a. Statutory and standards-based access to medical data. Personalised medical data in the health information system must be protected from irrelevant people (ISKE S2). Users must be identified for the purpose of data processing and the data must remain confidential during storage and transmission.
    b. Releasing data with the data subject's consent. Data subjects have the right to publish data concerning themselves. Data protection limitations cannot be applied to the digital services the data subject uses to publish (process, view, present or transmit) data concerning themselves. At the same time it is possible to assist users in choosing the safest solutions by registering and publishing digital service security certificates.

3. A digital service interoperability certificate. Exchanging data between digital services requires agreement on the definition and format of the data. Verification of honouring these agreements can be solved in a number of ways.

  a. The integrator’s responsibility upon managing data exchange. Automatic control of data added to the health information system.
  b. The user’s responsibility upon choosing a digital service. Digital services verify data when data is issued from the health information system. Digital services can use data to the extent that the data correspond to agreements and the digital service follows interoperability agreements.
  c. Conformity assessment of digital services to data standards. Similarly to the security conformity model (ISKE), whether digital services correspond to the conformity profile is also checked.

Classification of digital service certificates and specification of the procedure for awarding them are prerequisites for a functional digital service market.

4. Interfacing activities of digital services

One of the main expectations of digital service providers is the existence of a comprehensible interfacing process with predictable costs. Based on the current EHIS legal system and interfacing experience, a schematic overview of interfacing is provided in the case of two different use cases.

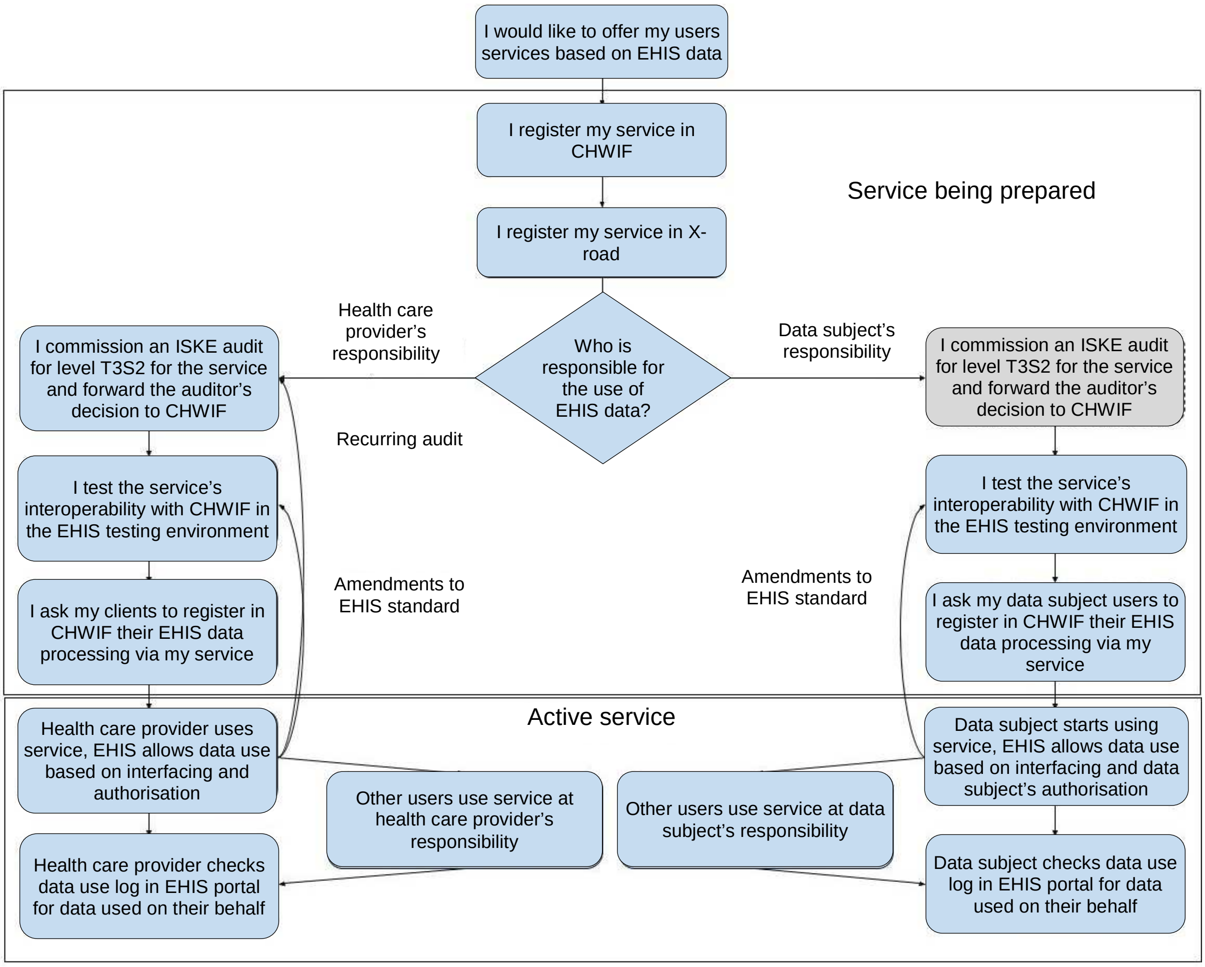
1. A digital service provider wishes to offer services to health service providers. Digital service also includes adding data to and reviewing data in EHIS.
2. A digital service provider wishes to offer services to people. Digital service also includes reviewing data in EHIS.

The following steps are taken in the case of both use stories:

1. Registration of digital service and initiation of interfacing process
2. Registration of the X-road identity of the digital service
3. Security check of the digital service and registering audit results
    a. Applications processing data at the data subject’s responsibility do not require a high security level. Digital service providers can undergo a security audit voluntarily to win users’ trust.
    b. Applications adding data at a health care provider’s responsibility are required to prove they meet high security standards.
4. Testing the interoperability of the digital service and registration of interoperability
    a. Different digital services have different interoperability requirements. For example, digital services which can only be used to send out referral letters need interoperability confirmation only to the extent of the referral letter standard.

    b. The interoperability check of digital services adding data must ensure high enough quality for the medical data added.

5. Registration of digital service users
    a. The health care provider gives the digital service provider authorisation to read and write EHIS data on the health care provider’s behalf.
    b. The data subject authorises the digital service to read the subject’s EHIS data
6. Allowing use of EHIS data via the digital service
    a. Allowing data use at a health care provider’s responsibility (authorisation) is based on a health care provider’s active licence, secure data exchange channel, digital service certificate of data security and interoperability and the digital service provider’s authorisation granted by the health care provider. If necessary, it is checked whether there is a therapeutic relationship between the health care provider and the data subject.
    b. Issuing data at the data subject’s responsibility from EHIS is based on a secure data exchange channel and the digital service provider’s authorisation granted by the data subject.
7. Should the digital service terminate operations (due to liquidation, restructuring or bankruptcy) it shall be demanded that they complete data security-related actions.


I would like to offer my users services based on EHIS data
I register my service in CHWIF
Service being prepared
I register my service in X-road
Health care provider’s responsibility
Who is responsible for the use of EHIS data?
Data subject’s responsibility
I commission an ISKE audit for level T3S2 for the service and forward the auditor’s decision to CHWIF
I commission an ISKE audit for level T3S2 for the service and forward the auditor’s decision to CHWIF
Recurring audit
I test the service’s interoperability with CHWIF in the EHIS testing environment
I test the service’s interoperability with CHWIF in the EHIS testing environment
Amendments to EHIS standard
Amendments to EHIS standard
I ask my clients to register in CHWIF their EHIS data processing via my service
I ask my data subject users to register in CHWIF their EHIS data processing via my service
Active service
Health care provider uses service, EHIS allows data use based on interfacing and authorisation
Data subject starts using service, EHIS allows data use based on interfacing and data subject’s authorisation
Other users use service at health care provider’s responsibility
Other users use service at data subject’s responsibility
Health care provider checks data use log in EHIS portal for data used on their behalf
Data subject checks data use log in EHIS portal for data used on their behalf

4.1. Recommendations and next steps

The drafters of this report **recommend choosing a combined scenario** where risks and impact are balanced by the private sector, the state, personal responsibility and openness to new technologies. Hence we recommend scenario **BCG-combined**: B1, B2, B3, C1 and G.

B1: how can HCPs be motivated to involve more new technologies and service providers to provide new solutions and solve their own services? The state finds economic means to involve private investors' money and increase health insurance funds to integrate new solutions with health care ('innovation foundations'). For instance, when the state decides that besides the agreed price and efficacy variables the result of treatment and quality indicators are also taken into consideration when treatment is funded and priced, then services built on collected data and digital services are of great use in connecting various treatment stages, including follow-up treatment, rehabilitation and survival. Also the examples in the Annex.

B2: outsourcing various roles and activities related to HIS administration and development, leaving the state (MoSA+CHWIF) with the role of service market supervisor and regulator. For example, moving the standardisation service to the private sector, where the services of the state, HCPs and DSPs must follow the standards and the standards require a fee (similar to international standardisation organisations). Another similar certified third party could provide authorisation and procedures for accessing a data warehouse (or data repository) following the established and approved regulations.

B3: people or patients buy private services themselves and can also reuse data collected in HIS (mainly global services).

C1: people use their HIS data to buy paid services and health services at their own responsibility. People buy various technologies and services from both the local and global markets for managing risks, prevention and buying treatment services from insurance companies.

G: Global-oriented – the state promotes the development of global services by combining different scenarios. It is recommended to combine opening up the market to the private sector and attracting innovation and investors' money with an international project to introduce a project that may interest the global market, for example creating personal health accounts for the residents of Estonia and e-residents with the aim of influencing the international standards market. This opens up an opportunity for the private sector to offer standardisation and data warehousing operator services along with respective authorisation. This scenario also gives people more options to use global services along with an increase in their own contribution (and freedoms).

Estonia's e-health vision should be based on ambition to participate in the creation and design of international e-health standards, at least in terms of the EU common market.

Depending on which combination or balanced combination between different parties and policies is chosen, it will require a detailed analysis and more precise planning.

Thus the next steps in terms of further activities are:

- decision on scenario choices in the longer term – drawing up a vision – global or local service?
- creation of a portfolio of outsourced services and describing criteria for future operators

    - standardisation service
    - data access (management of people’s authorisation) certification service
    - access authorisation service for third parties
    - requirements for certification of devices and services and procedure for publishing
    - establishing legal presumption for launching operator services and paid services
    - public procurements to find service operators

- Describing CHWIF service portfolio (to people and companies) and launching services
    - interfacing regulation procedure
    - data issuing procedure
    - specifying technical solutions of services and procurements