‘Being diabetic in 2011’

Identifying emerging and future risks in remote health monitoring and treatment

ANNEX I – *Scenario Building and Analysis Template*

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For more information on the EFR Framework, you may contact:

Barbara DASKALA Barbara.DASKALA@enisa.europa.eu
Dr. Louis MARINOS Louis.MARINOS@enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2009

Structure of the template

The template is structured as follows:

- Introductory part, where a general overview and the background of the scenario idea is provided

- The Scenario description, including the following information:
  - *Scenario type*: explorative or predictive [in our case it is predictive]
  - *Scenario raw description*: this is where we the scenario is described in free text.
  - *Assumptions*: Any assumptions made while formulating the scenario.

- "Framing the scenario" section contains a number of fields, with information we would like to know. Since as you will see most of this information required may be already included in the raw description, this section is actually offered as an alternative, in case experts instead of providing a free text, rather prefer to introduce their input directly to a more structured template.

- "Analysing the scenario" section: this is where the Scenario Analysis takes place. This is actually a borderline between the actual scenario analysis and risk assessment of the specific technology / applications we have chosen. We have included methodological items we would need to consider in order to perform the assessment (such as assets, threats, vulnerabilities, impact etc).

- A Glossary / Aid, where important terms like "threats", "vulnerabilities" etc are defined.

- Other information, where more information not specified in the table above could be specified, or figures and picture added etc.

- References, where all references used for the completion of the tables should be listed.

EFR Application Scenario – "Remote Health Monitoring and Treatment"[1]

Recent advances in information and communication technologies (ICT), miniaturization of sensor devices and computers, as well as the wider availability of connectivity and wireless networks gives rise to a number of services and applications involving wirelessly connected sensors and actuators in a body area network (BAN), personal area network (PAN) or in the environment. The miniature sensors and actuators are in turn connected via the Internet to a number of back-end information systems. These systems collect information used by a number of ICT systems of different parties offering different (integrated) services.

The trend towards more integrated systems and the inclusion of BANs and PANs in these networks generate application and business opportunities and impact industries, users and service providers in different domains. For example, in the healthcare domain, patients as well as healthy people concerned about their wellness will be able to obtain medical advice wherever they are, based on data captured instantly by sensors in their body/personal area networks. These systems span a range of applications, from remote patient monitoring and treatment, via tele-surgery and emergency care to remote elderly care. They can be applied in different locations, from hospital to home, as well as on the move and are meant for a range of ages, from childhood to the elderly implementing and embedding pervasive healthcare in people's lifestyles. Sensors will continuously measure bodily parameters such as blood pressure, weight, movement and glucose levels and make these available to medical professionals.
These systems typically comprise (wireless) sensors worn by the patient that report results through a local hub which in turn forwards them to a server from which the medical professional can retrieve the results.

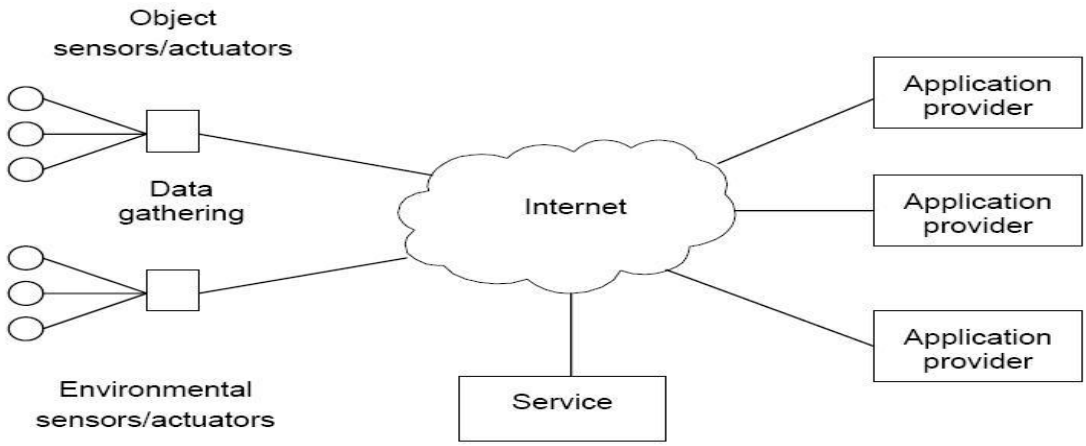

Figure 1 General architecture

[1] The text and the graph presented here are written by Milan Petkovic, Philips Research and have been submitted to the ENISA Stakeholder Forum.

Although the applications above differ, they can all be operated on a similar network infrastructure. Figure 1 shows a high-level, abstract view of a network infrastructure. It shows that there can be sensors and even actuators in the environment (e.g. home, road, …) or on/in objects (persons, cars, …), which communicate wirelessly to some data-gathering station which subsequently can communicate with applications on back-end IT systems or with services on the Internet which are used by the applications.

A remote patient monitoring system, depicted in Figure 2, is an example of such an end-to-end system. From left to right, we see that a person can be monitored by wireless sensors on his body and in the environment. The data collected can subsequently be sent to a service provider running the remote patient monitoring application.

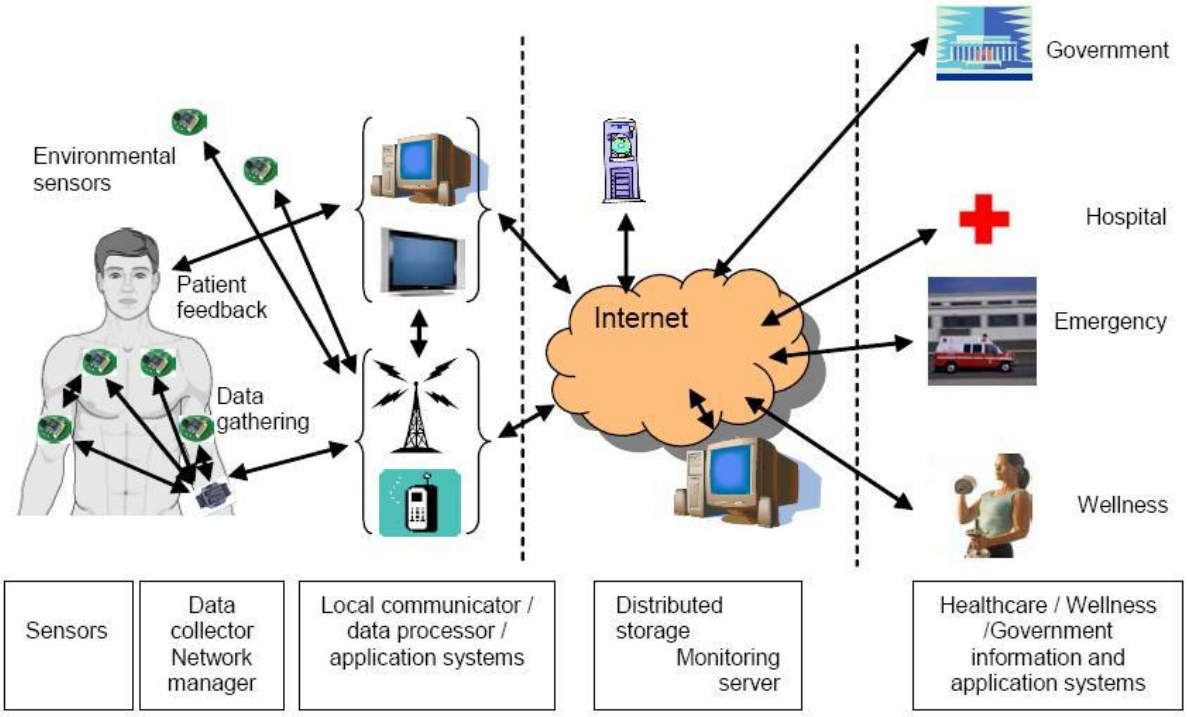

Figure 2: An example of a remote patient monitoring system

These data are stored in a remote patient monitoring server. The remote patient monitoring application may then interface with applications and IT systems of different health and wellness providers.

"Being diabetic in 2011"[2]

Type of scenario flow *["predictive" or "explorative" to indicate the nature of the scenario]*	*Predictive*: what will happen
Raw description of scenario [*who does what* or *what happens*]	
Ralph is a 58-year-old professional with type II diabetes. He is hypertensive and overweight and he has enrolled in a newly-established diabetes management program. As part of this program, Ralph maintains an online health journal to record trends in his health status. On a daily basis, his glucose measurements, nutrition, weight, blood pressure, and pulse rate are recorded using special gadgets, which are provided to him by the hospital upon enrolment in the program; Ralph pays only a limited contribution to receive them, since the rest is covered by the insurance scheme he is covered under. He receives reminders from his mobile, to perform certain activities and to take his prescribed medication at designated times. At the same time, he receives feedback (for example via phone or sms) from his physician on his progress and information that helps him manage his health more effectively. Secure access to this service is provided by a health card, which also maintains an up-to-date version of his emergency health data set. Ralph and his family physician have agreed in advance that more detailed information about Ralph's health status will be provided to the call centre for Ralph's safety. In his last visit to the family physician, she prescribed medication for the hypertension and she strongly suggested a health plan that includes regular exercise supported by remote monitoring and treatment. For his convenience, these exercises can be done at home or while on the move, in collaborating gyms. However, it is important that they are performed regularly and correctly. Ralph's new health plan provides him with access to a call centre, where health professionals periodically review his exercise program (upon his request) and manage alarms on a 24/7 basis. Every morning, Ralph logs onto his health journal using his health card. He is reminded of his morning health management routine. As part of his daily morning routine, he takes his medication; he measures his blood pressure, pulse rate, glucose levels and weight, which are recorded in his health journal. The devices and other home sensors communicate with the home hub and through that data is transferred to Ralph's online health journal. The data is analysed automatically, trends are computed and Ralph receives feedback which is both auditory and visual (images) on his health status. Then, he proceeds with his morning exercise routine. His family physician has provided him with a rather demanding health program with set intermediate goals. Before Ralph starts his exercises, he puts on a special garment with embedded wireless sensors. A patient-monitoring system checks the quality of the performed exercises, and progress towards his goals. The sensors monitor the exercises and their measurements	

[2] *Based on Philips Research scenario submitted by Milan Petkovic and further developed by Ms Catherine Chronaki of FORTH Institute.*

are processed for feedback to Ralph (he may get automatic instructions) and for information to his health providers via the monitoring center. During the regular routine, information related to the practice of the exercise, but also to Ralph's health status, is recorded in his health journal, and transmitted to the call center, where health professionals review them, and create a patient monitoring report for Ralph and his family physician as prescribed by the health plan. The report then becomes part of Ralph's health journal.

Both Ralph and his family doctor are confident that Ralph is safe while he exercises and that if an emergency problem was to arise, it would be handled efficiently and effectively. In rare cases, an acute medical problem may arise during the exercise, which is picked up by the sensing nodes of the garment, which are continually monitoring his biosignals. If this were to happen, the system would raise an alarm and urgently notify Ralph and the call centre, which in turn would evaluate the alarm and depending on its severity inform his family physician, emergency services and possibly his next of kin.

Ralph has a busy professional life and travels a lot, so he has agreed with his doctor that they carry out their bi-weekly medical visits through video-calls to be sure that Ralph remains healthy and responds well to treatment. They set up the medical tele-consult using an online appointment-setting service, which identifies a time convenient for both Ralph and his doctor who are then notified when that will be. They can use a laptop or mobile-phone for the consultation, during which Ralph's family physician checks Ralph's progress and examines his up-to-date electronic health record (EHR), which contains data from the hospital, Ralph's patient monitoring service and his health journal. Ralph has consented that his doctor and the hospital be granted access to his EHR. He can decide how much access and to which parts of his EHR, they and other specialists (support staff, pharmacies, his employer, insurance company and others) may have. Ralph's EHR indicates trends and possible alerts that the doctor may correlate to Ralph's medication and ongoing treatment. A record of the tele-consultation and the doctor's comments become part of Ralphs' health record. If the doctor decides that a change in Ralph's medication is warranted, he can use the e-prescription service to send the revision to the pharmacy near Ralph's home where he usually picks up his medications.

All in all, Ralph feels rather happy with this technology as it is very convenient to him (he doesn't need to leave his home) and he knows that if a problem occurs he is helped on the spot.

Assumptions

[any assumptions made while writing the scenario flow. Assumptions is a place holder for information that may concern generic information about relevant legislation, devices, applications, participants, etc.]

1. Connectivity between medical sensors/devices, gateways/hubs and healthcare services is present.

2. Health professionals rely on accurate data coming from certified devices. Patient safety is most important, but privacy is also taken care of, as required by legislation (EU Directive 46/95, HIPAA, etc.), e.g. personal health data can be used based on patient consent, only for certain purposes, on a need-to-know basis by certain healthcare providers (e.g. a doctor that has a care relationship with the patient).

While EU directives are important in terms of medical data, they are not exhaustive in terms of different regulations for medical data within member states. Even with regard to privacy legislation itself, while EU directives provide a baseline, some member states go beyond mere compliance with directives. Similarly while consent is a universal principle it is not applied uniformly or regulated uniformly across the EU. Substantial variations exist for example between new member states and the UK and Holland. While it is difficult to include all of the variations within one scenario, perhaps some acknowledgment of these variations is necessary, or the selection of one regulatory approach as an exemplar of best-practice for the scenario.

3. For the purposes of this scenario and the analysis that follows, the existing legislation and regulations regarding Data Protection are considered.

4. Upon enrolment in the disease management program, Ralph is duly informed about the whole process, also in case of emergency, and especially about the risks that the latter case could entail. He is also required to sign an agreement with the hospital.

5. This information can be collected by different sensors and medical devices such as blood pressure meters, ECG (electrocardiogram) devices, etc. Health professionals need to be able to verfiy and trust the origin of that data (to be sure that it comes from Ralph) as well as which device was used to produce the data (some patients may be using less or more accurate devices).

6. Sometimes, health professionals are also concerned with the quality of measured data as some patients are not able to produce reliable measurements. Therefore, the measurements often come together with quality indicators that help the health professionals judge whether remote measurements are reliable. Based on such detailed information about Ralph's current health status the doctor is able to take adequate measures.

7. There are quality assurance procedures in place in the hospital that are followed for the disease management programs. Staff are provided with training to familiarise them with these procedures.

8. The existence of an infrastructure to support ePrescription services in European states, is assumed. Such services are now being rolled-out in some countries such as Denmark and soon the Netherlands. This fact implies the existence of a medication record (typically part of the EHR) and connectivity of the family doctor with the pharmacy, and the insurance fund.

9. The deployment of interoperable health cards that include an emergency data set and provide access to health services while abroad, is also assumed. This health card possibly in combination with biometrics is used to protect the identity and data of Ralph.

10. The existence of a public key infrastructure that provides among other things secure signing of information assets e.g. health monitoring reports and prescriptions, is assumed.

11. The home hub is a PC-based device that is connected to the Internet and has wireless connectivity with the measurement devices (BPM, etc.)

12. It is assumed that Ralph does not suffer from technophobia or dementia and that he is a self-aware and active patient who does not resist persistent self-monitoring.

13. We assume that technical devices can communicate enough information to 'take adequate measures' (or at least that they communicate enough information to decide when a personal consultation is needed).

14. Ethical issues are not considered within the scope of this scenario, and so no details are included regarding ethical matters or relevant stakeholders (such as the Hospital Ethics' Committee). However, it should be noted, that ethical considerations may be identified in the course of the analysis.

15. Considering three major possibilities in healthcare models, namely: (a) Public health care provision (government or employer pays), (b) Private health care provision (Ralph pays himself), (c) Mixed model (part is paid by Ralph part by insurance company, private or public), we assume that for the purposes of our scenario, a mixed model is followed, with Ralph making some (limited) contribution to his health expenses.

Framing the scenario	
Timeframe [*when the scenario takes place]*	2-3 years in the future
Location [*where: Home / work / public space…*]	• Home, work, hospital, medical office • On the move (fitness, jogging, etc.)
Actors [*who: entities relevant to the scenario and describe their roles and goals. These most probably include humans*	• Patient (Ralph) • Ralph's family members and friends, whose privacy may be affected and/or who may be enlisted to implement the self-monitoring system • Family physician (GP treating Ralph) • Hospital/medical practice • Data centre: Is an organisation that offers various services around health monitoring and operates the IT systems (HW, SW). It can be a disease management organization, a hospital, or a specialised company. This is the most important actor in a remote patient monitoring system. Basically it operates the back-end server. It

and organizations and NOT IT systems.]	collects the health data from patients (taken by their measurement devices or their subjective data). It implements some logic procedures that interprets the data (show problematic cases, trends, etc.). The IT applications of the data centre provide normally a client application (often thin web client) to nurses/doctors at the call center. They can upload a care plan for each patient and manage these accordingly. • Call centre: it is staffed typically by nurses and other specialized health professionals and it operates 24/7. The call center staff are allowed to contact the subscriber, their family physician and ambulance services in accordance to the alarm level as reported by the remote sensors. In the prospective scenario, the call center has access to biometrics and the health profile of the subscriber. • Emergency services: Is an organisation that is responsible for emergency medical support at the location of the patient and the provision of transportation to hospitals/doctors. • Pharmacy • Insurance company • Gym • Internet Service Provider • Mobile communications Service Provider • Scientific research medical institutes (interested in the application field and processed data) • Pharmaceutical companies (interested in the application field and processed data) • The governmental department responsible for public healthcare • Ralph's employer and/or business partners who have a stake in his functioning Around the Data and Call Centres, various health services can be developed. The number and nature can vary significantly. The involved service providers might have service level agreements (SLAs) among each other. Some examples are: • Health Plan Service Provider (SP) • Diabetes management program SP • Health journal (Personal health record) SP • Appointment SP • Medical visit through video call SP
Technologies / devices [*technologies / devices used in the scenario*]	• Special garment with embedded sensors. • Data collector/ Home Hub: This can be an application running on a PC, multimedia center, setup box, mobile phone, PDA, Intel health guide device, special medical hub device, etc. This device might be a normal PC, set-top box or Intel PHS6000 (btw. with integrated camera allowing for two-way video calls). Further components of this device might be:

	- Windows/Windows mobile/Linux/Embedded system OS - Multi-user device - can authenticate users (user name/password, biometrics, etc.) - Encryption capabilities, maybe even password protected HD, support of SSL towards the backend system - Could deploy a DBMS with authentication/authorization/auditing mechanisms to store data locally. • Hospital's IT system: Usually, this is a different IT system (e.g. hospital information system – EPIC is an example) that can recieve the data via email or using specific protocols (e.g. HL-7) from the remote patient monitoring system. Components of this IT system might be: - All physical and IT security mechanisms applicable to traditional data centres (fire walls, intrusion detection, antivirus, etc.) - Provides remote access to patient data from the call centre (often a thin client over a VPN) - Authentication (login/pass), role-based authorization - Data exchange between the call centre and GPs often by normal email, rarely a thin client provided to the clinicians over VPN. • Medical and fitness devices such as blood pressure meters, ECG device, activity monitor, Weigh scale, pulse rate measurement, etc. These devices include a processor, storage space, wireless (PAN) interface to connect to the PC or other mobile device; cable connector (USB) to connect to a computer or similar device. Wireless connectivity (e.g. Bluetooth, pairing protocols). Captured data is downloaded to a PC or other computing device using one of the interfaces. This transmission is not encrypted. Device ID (e.g. Unique Serial Number) is transmitted with the date (helping identify data quality parameters, but also creating privacy concerns). Data on disk are not encrypted or otherwise protected. It can be read and modified by any device that can read external storage devices. Storage space is limited, and older data drops off the list. Data items are typically time stamped. Often there is unidirectional communication. • Telephones and videophones. These devices typically have several wireless interfaces (infrared, Bluetooth; both not protected) and a wired USB interface (also not secure). Voice communications are scrambled. The device has two unique identifiers that can be linked to

	subscribers (in GSM, EMEI (device ID) and IMSI (subscriber ID). IMSI is substituted with session IDs during some operations. The device has a full operating system, that is, however, not very secure. The device has significant writable storage that is not strongly protected and can be read by any devices capable of reading external storage. The OS and applications are susceptible to malware. SIM card can be moved to another device. The device can frequently be used with a different SIM. Lost and stolen devices can lose communication privileges, but storage will continue to be accessible. Devices can be synchronized with PCs and similar devices; passwords and other credentials may be stored in the mobile device. Firmware in the device can be changed (in a way not visible to users). • Digital camera [similar in storage protection, interfaces, synchronization mechanisms to other devices already described]. • Networks (wireless, PAN, TCP/IP) – Wireless networks are susceptible to interceptions; both WEP and WPA have been broken for Wi-Fi. • Encryption, authentication, Identity management, record management. • Data translation (in the required formats), aggregation, and analysis technologies. • Other IT-Equipment used in the interaction between actors: It is assumed, that additional IT-Equipment will be used in the interaction between actors. Patients, for example, might use private PCs/Laptops to communicate with their physicians (i.e. Patient IT-Equipment) while doctors might communicate with other experts via their desktop PCs (Doctors IT-Equipment). • Health card: This is usually a token (i.e. based on Microchips), that performs strong authentication (including signatures and encryption) and also has some secure storage to store sensitive medical data. • Bluetooth Medical Device Profile Specification (see http://www.musenka.com/info/doc/MDP(MedicalDevicesProfile).pdf) • USB Personal Healthcare Device Class Specification (see http://www.usb.org/developers/devclass_docs/Personal_Healthcare_1.zip) • ISO/IEEE 11073-10417 (Glucose) • Continua xHR Interface
Applications	• Patient monitoring service (disease management)

[*applications used in the scenario*]	• Electronic health record system • Health plan • Audio Visual Conference (tele-consult) • Online appointment scheduling • ePrescription service • online appointment scheduling • Health journal service
Data *[information that is collected, or flows through the network, or is being stored and further processed]*	• Electronic health record • Health plan • Health journal: a personal health record linked to Ralph's health plan where he records his daily activities, and data from various medical devices • Health monitoring report: Based on the biodata collected from various devices and Ralph's own remarks a summary report is compiled on a daily/weekly/biweekly basis. Ralph's family doctor, reviews it during the medical-televisit, and possibly uses it as input to his own report. • Prescription • Identification Data: As identification data we consider any data used as means of unique (electronic or otherwise available) identification of actors or assets in the domain of the e-Health system and its users. • Digital signature • Emergency Data set • Medical appointment • Alerts of various types • Reminder of various types • Health trends • Health data: vital signs, blood pressure levels, blood glucose levels, pictures of skin and feet • Device specifications
Drivers *[key drivers behind the scenario: socio-economic, political, environmental or personal motivation...]*	• Improve quality, effectiveness and efficiency of healthcare for everyone. • Convenience for patients. • Increase quality of life for professionals on the move. • Decrease costs of healthcare. • Profits for the healthcare industry (because of early detection more people will be treated, which does not necessarily decrease costs, but may rather increase them instead...) • Profit for the companies that produce the technologies. •

Analysing the scenario

A. Assets

[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
Intangible				
A1.	Health / Life	Refers to the physical and psychological condition of an individual; his/her physical and psychological well-being and absence of disease.	Patient / Person	10 – Its importance is self-evident; inadequate protection will result in deterioration of an individual's health and may lead to deterioration or loss of life.
A2.	Autonomy	Autonomy is a varied concept, for the purposes of this scenario autonomy can be seen as the right of the patient to exercise control over the data collected to them. It also refers to the patient being given more control over their treatment decisions and medical encounters as part of a move towards individual responsibility for health care.	Patient/Person	10- Autonomy is a critical concept in the EU. It is reflected in fundamental charters on rights, data protection legislation as well as ethical guidelines dealing with patients, medical professionals and the relationship between them.
A3.	National Healthcare System	The system with which the state provides healthcare and medical services to people at a reasonable cost.	State / Citizens	10 – It is very important to have a good national health care system in place, in order to ensure the provision of quality health services at a reasonable cost. Again, improper operation of the NHS may lead to deterioration in the quality of or even loss of human life.
A4.	Human rights and social values	Human rights and social values, e.g. Privacy, Non-Discrimination, Dignity, social inclusion, trusted human relationships and e-	Patient / individual, family, friends, society in general	10 – It is imperative to protect those rights and social values from violation. Violation of these rights has a huge potential impact. Damage to these rights would lead to mistrust and a loss in

Analysing the scenario				
A. Assets *[tangible or intangible: any devices, technologies, applications, processes, data of value]*				
No.	**Asset**	**Description or reference to above described elements**	**Owner** *[involved actors / organisations]*	**Perceived Value** *[Scale 1-10 with some motivation about selected value]*
		inclusion etc.		confidence in the system and those involve in provision of the system

Analysing the scenario

A. Assets

[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
A5.	Mobility of people	The ability and potential of people to move across countries and be provided with the same quality of service, in our case Healthcare service.	Patient / individual, doctors / health professionals, people in general	8 – Mobility of people is an important requirement especially in our information society. Similarly the guarantee of freedom in mobility is a fundamental element of the European Union.
Tangible				
A6.	Health card	Contains emergency data set, used for authentication, possibly also for verification for services	Patient, doctor, Service providers	8 • Access to the service can also be achieved by other means. • Data are assumed to be encrypted. • Currently only a small set of data is included. • Medical professionals are obliged to verify the data through medical examinations.
A7.	Health monitoring devices: - Garment with biosensors - Blood pressure monitor	Worn during exercise, taking measurements and transmitting them to the patient monitoring call center through home hub. Measures blood pressure, sends measurements via Bluetooth or USB or WIFI to Home Hub Measures weight, sends measurements via Bluetooth or usb or WiFi to Home Hub Measures blood glucose levels, sends	Health monitoring call center SP, health journal SP	9 – Important in order to function but easily replaceable. Integrity/ quality of the supplied measurements have the potential to seriously affect the health andlife of the patient. Data needs to be reliable and trustworthy in the eyes of health care professionals and patients

Analysing the scenario

A. Assets

[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
	- Weighting scales - Glucose meter	measurements via Bluetooth or usb or WiFi to Home Hub		
A8.	Data collector / Home Hub	Device at the patient's home, communicating with all the external networks and devices.	Patient	10 – It transmits and stores all the necessary personal or medical data of the patient. Critical device without which the system cannot operate
A9.	Personal IT equipment	The IT equipment the patient uses at home in order to participate in the DMP. This may include laptops or workstations, digital cameras, telephones and videophones of patient or doctor / health practitioner.	Patient, Doctor, Health practitioner, Patient, health journal SP, mobile phone SP	8 – It may contain personal and sensitive data, used as access points to the service; plus availability of the equipment is also important.
A10.	Data centre and call centre	Critical provider of the remote health monitoring system. Is the gateway between the patient and doctor. Responsible for recording and providing analysis of remotely generated data. Also responsible for providing responses in the case of emergencies.	Data and call centre operators	9 – Important to operate appropriately, since the whole delivery of the RPM service is heavily based on their proper and continuous function.
A11.	Electronic Health Record	Contains health information confirmed by health professionals including prescriptions and personal data.	Patient, Call Centre, Hospital, Medical Staff	10 – Can be varied, depending on the exact data that is collected, but in most cases considered very high. Personal data gathered by sensors may provide other information for example location. As demonstrated

Analysing the scenario

A. Assets

[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
				in Sweden's Lindt case, medical data which has personal data linkages is not protected in some instances. (i.e. Ralph might be involved in a crime, his location at the time might become directly relevant data for an investigation and could be extrapolated from the data of the sensors).
A12.	Health Journal	Records health measurements, personal data, analyses trends, provides feedback, data are reviewed by doctors and some can be consolidated and accepted into the EHR	Patient, health monitoring call center	10 – Depending on the exact data collected and stored in the journal, but in most cases is considered to be high [10]
A13.	Electronic Prescription	Prescription new or repeated sent to the pharmacy and the insurance provider for reimbursement. Includes personal data and a summary of the diagnosis to justify the prescription.	Pharmacy, insurance fund, Family Physician, medical practice, patient	10 – Prescription may provide some personal or health data, and its integrity is important in terms of potential mortality of patients participating.
A14.	Public health research data	Easily available data enables extensive epidemiological research	Public health research institutions, governments, …	9 - The availability of abundant data for public health research is one of the major pros of this technology. There are important considerations in relation to data protection and informed consent in making use of such data.
A15.	Medical Procedures and	An important element of the scenario is the assumptions in place regarding the	Call Centre, Medical Centre, Medical Staff	**9 –** Knowledge and expertise in terms of the deployment of the technology would appear to be vital to its success as well as ensuring

Analysing the scenario

A. Assets

[tangible or intangible: any devices, technologies, applications, processes, data of value]

No.	Asset	Description or reference to above described elements	Owner *[involved actors / organisations]*	Perceived Value *[Scale 1-10 with some motivation about selected value]*
	Operational Standards	procedures and operations followed by medical staff. However it's not clear how these are designed and how their quality is guaranteed prior to the technology being deployed, during its operation and what sort of monitoring systems are in place for the medical staff.		the safety of the patient. The necessary skills may not be widely present within medical professionals and may involve as a result training for medical professionals in the use of the technologies.
A16.	RPM Service / Disease Management Program	Service described in the scenario	DMO	10 – No service means no care, and no care would entail potentially serious health problems for individuals.
A17.	Hospital IT System	Will store data relevant to the individual, including the EHR and forwarded analyses from the call center.		9 – Important to operate appropriately, since the delivery of the RMT service is heavily based on it. The EHR is stored in this system.

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
V1.	Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System	High. The service, components, special equipment or interfaces to other systems may fail to take into account all the aspects of the problem they need to solve. Generating the possibility of malfunction or other problems of unknown magnitude.
V2.	Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program	Medium to High. eHealth industry will push a lot of devices and services onto the market (technology push). Their acceptance, but also their effectiveness will depend on usability and limitations on the burden put on the patient through remote monitoring.
V3.	Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program	High. Critical parts of the monitoring /treatment process will depend on patients rather than specialised/expert professionals. Patient must be cooperative, follow medical instructions and use the devices appropriately and diligently
V4.	Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure	A13. Electronic Prescription A16. RPM Service / Disease	Medium. Importance of connectivity and interoperability of existing and future devices and information management

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
	communications, digital authorisation, eID, etc.)	Management Program A3. National Healthcare System	systems. Depending on the operation of hub systems.
V5.	Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment	Medium. The equipment is used in environments that do not offer a uniform level of physical and logical protection in contrast to the controlled environment of a hospital. As such the equipment may be exposed to several threats ranging from environmental imposed damage (lighting, moisture, corrosion, fire), patient accidentally dropping the equipment through to misuse and theft. Coupled with the absence of safeguards such as anti-theft protection for the device or mobile storage, anti-shock protection, would enable a series of threats.
V6.	Lack of interoperability between devices and/or technologies and/or systems	A6. Health card A7. Health monitoring devices A10. Data centre and call centre A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program	Medium. Importance of connectivity and interoperability of existing and future devices and information management systems. As well as the interoperability of complementary services and systems. Systems which are not inter-operable may hamper the efficiency of the system operating in different places, contexts and environments.
V7.	Multiple actors (patient, SPs, call center, etc) have access to data	A8. Data collector / Home Hub A10. Data centre and call centre	High. Data needs to be accessed by many different actors, having different authorisation levels and may be used in quite

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
		A16. RPM Service / Disease Management Program A15.Hospital IT System	different contexts. Assigning the right authorisation will be very complex. This will in turn make data management a difficult task
V8.	Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub	Low to Medium. Because of time pressure to market devices as soon as possible and offer them at cheap prices, the devices may end up providing low quality output or support a limited set of functionality (e.g. not provide multiple patient support, or provide measurements of lower accuracy). Also, the limited hardware capabilities of the device needs to be considered within the scope of this vulnerability.
V9.	Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System	Medium to High. Devices communicate over unprotected channels or publicly accessible channels (Infrared, Internet, radio signals, i.e. Bluetooth) which are exposed to more threats due to the vulnerabilities of the medium.
V10.	Lack of or inadequate identification & authentication controls	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System	Medium to High. Lack of appropriate identification and authentication controls may lead to unauthorised access to important personal and/or sensitive data.
V11.	Lack of or inadequate logical access control	A7. Health monitoring devices A8. Data collector / Home Hub	Medium to High. The RPM is a complex service including many components exchanging information. These exchanges

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
		A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System	occur through several types of interfaces for user to user, user to system and system to system interactions. Given the nature of the data (medical and personal) these interfaces need to be highly secure and make use of strong access control mechanisms
V12.	Lack of or low awareness / Training in 1. Information security 2. IT 3. RPM system and equipment 4. pertinent regulations and legislation (e.g. data protection)	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System	High. Actor knowledge, whether patient or medical professional, about the operation of the equipment, the service, IT infrastructure involved and the possible information security implications, will affect the acceptance and effectiveness of the system. Medical professional acceptance may also be an issue where some medical professionals either ignore the remote data, considering it not reliable, or do not trust the remote nature and aspects of the system.
V13.	Unmanaged IT Equipment 1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment	Medium to High. Equipment not under the direct control of the RPM service organisation will not receive regular professional (IT) monitoring and maintenance. This means configuration may not be secure or appropriate, security updates may not be installed, programs from unverified sources may be installed and the integrity of the system is not verifiable.

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
V14.	Unencrypted Data Storage	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System	Medium to High. Data used in the RPM, most of them are of high value, may be stored in several temporary locations before reaching the RPM Data center (e.g. measurement device, communication hub, data collector device). In addition some will need to be shared with medical professionals or hospitals and will be stored in the respective IT systems for a shorter or longer period of time. Usage of unencrypted storage in all of these places allows for the potential of several threats.
V15.	Wireless networks security shortcomings 1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment	Medium to High. Wireless networks have inherent difficulties in addressing security starting from the obvious one which is the broadcast nature of the medium favouring potential eavesdroppers. In addition many of the security protocols used to overcome these inherent problems have proven to be inadequate and obsolete in a relatively short period of time.
V16.	Lack of common legislation / interpretation in EU member states.	A15. Medical Procedures and Operational Standards A3. National Healthcare System	Medium. Legislation in Member States is not uniform and not even static in areas such as data protection and privacy, cyber crime, etc This gap is even deeper considering social and cultural factors that lead to variations in the interpretation of laws. Thus it is extremely difficult to determine whether provision present in one MS will still be available or even

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
			possible when crossing the borders to another MS.
V17.	Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System	Medium. Patient consent has to be taken into account regarding the use of his personal and medical data. It is of extreme importance that the technical infrastructure of the service including applications, procedures, data classification and authorisation levels, provide the means to act in accordance with the consent provided by the patient. This holds also true for the ability of the interfaces with external systems, services, organisations to convey such information and the ability of such external entities to use and comply with the consent statement.
V18.	Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values	Medium to High. The statement the patient is required to sign is too intrusive, in the sense that it requires the patient to give his/her consent for access to data by more parties than it is required for the appropriate provision of the RPM service. The patient is therefore almost coaxed into giving his/her consent for his data to be disclosed or used by too many external parties.
V19.	Lack of data traceability; the patient cannot be aware when his data where accessed, by whom and why.	A11. ELECTRONIC HEALTH RECORD A15. Medical Procedures and Operational Standards	High. While the patient is asked to consent for the use of his data for specific reasons and by specified entities, he has no direct way of being notified on the occurrence of such processing and the exact entities and reasons for such access.

Analysing the scenario

B. Vulnerabilities
[of the tangible / intangible assets]

No.	Vulnerability Description	Asset(s) from the list above	Assessment [*High, Medium, Low with some explanation about selected level*]
		A16. RPM Service / Disease Management Program	
V20.	Different level of treatment in different countries.	A1. Health / Life A3. National Healthcare System A5. Mobility of people	Medium to High. Each Member state has a long established health care system that provides different types of service at different levels and cost. Mapping or provisions for counteracting these differences is not trivial even more since member states are either reforming or changing the nature of their health systems.
V21.	Huge amounts of data (personal and medical) collected and stored in databases easily accessible and linked / connected (data linkability).	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A16. RPM Service / Disease Management Program A17. Hospital IT System	High. Data can be mined for patterns that can be applied to uses not initially intended, communicated, accepted or even legal. They can be also used to create profiles while may lead to discrimination.
V22.	Complexity of medical data	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data	Medium. Individualised health care will depend on active and aware patients making informed decisions. A part of this will be making sense of potentially complex medical data. The system will counteract potential emergencies but there is a risk patients will continually mis-interpret their data, this

Analysing the scenario			
B. Vulnerabilities *[of the tangible / intangible assets]*			
No.	**Vulnerability Description**	**Asset(s) from the list above**	**Assessment** [*High, Medium, Low with some explanation about selected level*]
			could be exacerbated by poor care on the part of health care professionals.

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
C1.	Certification of devices used for measurement of health parameters	A7. Health monitoring devices A8. Data collector / Home Hub A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A3. National Healthcare System	
C2.	Compliance with regulation (data protection, privacy)	A6. Health card A7. Health monitoring devices A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System A4. Human rights and social values A5. Mobility of people	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
C3.	Data access is based on the need-to-know principle by adhered to by healthcare providers.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System A4. Human rights and social values	
C4.	User consent for processing and usage of personal and medical information. The user is informed about the entire (end-to-end) treatment process.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
		A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System A4. Human rights and social values	
C5.	(Medical) Device identification is used to ensure authenticity of interaction (i.e. measurements).	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A3. National Healthcare System A5. Mobility of people	
C6.	Quality assurance procedures	A10. Data centre and call centre	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
	are in place for the entire Remote Patient Monitoring and disease management system.	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A3. National Healthcare System A4. Human rights and social values A5. Mobility of people	
C7.	Quality indicators are used to help health professionals verify and judge the reliability of measurements.	A7. Health monitoring devices A8. Data collector / Home Hub A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A5. Mobility of people	
C8.	Health cards are interoperable and include emergency data sets acccessible while patients are abroad.	A6. Health card A11. Electronic Health Record A12. Health Journal A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
		A1. Health / Life A3. National Healthcare System A4. Human rights and social values A5. Mobility of people	
C9.	Health cards in combination with biometric data are used to protect personal and medical data of patients.	A6. Health card A11. Electronic Health Record A12. Health Journal A15. Medical Procedures and Operational Standards A1. Health / Life A3. National Healthcare System A4. Human rights and social values	
C10.	PKI infrastructure is used for authentication, generation of signatures (and encryption).	A6. Health card A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System A5. Mobility of people	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
C11.	IT components support encryption capabilities (e.g. SSL for secure communication).	A6. Health card A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System A5. Mobility of people	
C12.	Devices can authenticate users (e.g. by means of password and biometrical data).	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A3. National Healthcare System	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
		A5. Mobility of people	
C13.	Devices have strong authentication mechanisms (ref. to SIM based authentication of mobile phones or similar devices)	A6. Health card A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A3. National Healthcare System A5. Mobility of people	
C14.	Used DBMSs use authentication, authorisation and auditing capabilities for the processed and stored data (e.g. transaction security).	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System	
C15.	Operating systems of used IT-	A6. Health card	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
	Components support security controls: - Identification - Authentication - Access Control - Recovery - Logging - Automated updates - Encryption - Malware detection (viruses, malicious content, etc.) - Intrusion protection	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System	
C16.	Physical security controls for data centres: - Access control - Secure computing rooms - Redundant electricity /electrical circuits	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program	

Analysing the scenario

C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*

	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
	- Secure storage of backup media - Redundant air conditioning system - Flood protection - Service Level Agreements	A17. Hospital IT System A1. Health / Life A3. National Healthcare System	
C17.	Technical controls for data centres: - Managed SW and HW - Firewalling - Intrusion detection - Logging - Identification/Authentication - Encryption - Secure, redundant network connections - Use of VPN technology - Role based authorisation and access control	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A1. Health / Life A3. National Healthcare System	

Analysing the scenario			
C. Existing controls *[existing safeguards etc. already in place and that need to be considered. These may be found in the assumptions for example]*			
	Control Description	**Asset(s) and/or vulnerability concerned**	**Assessment** *[High, Medium, Low with some explanation about selected level]*
	- Backup/recovery - IT-Contingency - Service Level Agreements		
C18.	Trusted tamper resistance device with strong authentication mechanisms.	A6. Health card A7. Health monitoring devices A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A1. Health / Life A5. Mobility of people	

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
T1.	**Patient does not follow instructions for equipment use, treatment, medication.**	V2. Lack of usability/convenience and increased complexity or error proneness in the system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		High Given the complexity of the system patients may fail to follow/comply with all instructions they are given.
		V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		High
		V4. Excessive dependency on external infrastructures (e.g. existences of ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V12. Low awareness of 1.Information security	A15. Medical Procedures and Operational Standards		High

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		2. IT 3. RPM system and equipment	A16. RPM Service / Disease Management Program A3. National Healthcare System		
T2.	**Non-Compliance with informed consent legislation**	V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System		Medium to high. Poor informed consent could lead to situations such as: • Medical professionals routinely forget to check for the existence of patient's consent to save time or ease a difficult process. • Failure to explain procedures, data and operations properly to patient • etc
		V1. Flawed / inadequate design,	A6. Health card		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		inappropriate / incomplete implementation.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		
		V12. Low awareness of 1.Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
			A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data where accessed, by whom and why.	A11. Electronic Health Record A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and linked / connected.	A10. Data centre and call centre A16. RPM Service / Disease Management Program A17. Hospital IT System		
T3.	**Compromise of**	V1. Flawed / inadequate design,	A6. Health card		Low to medium;

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
	Credentials	inappropriate / incomplete implementation.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Patient passwords can be compromised through the secondary use of data, or just because the patient trusts or needs help to use a device/hub. Also Service staff that are repairing the hub can be seen as a trusted party etc.
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
		V9. Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V10. Lack of or inadequate	A7. Health monitoring devices		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		identification & authentication controls	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V12. Low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V13. Unmanaged IT Equipment 1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment		
		V15. Wireless networks security shortcomings	A7. Health monitoring devices A8. Data collector / Home Hub		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A9. Personal IT equipment		
T4.	**Breach of confidentiality and/or integrity. Eavesdropping/ spoofing/deletion on the interface between a medical device and the hub but also between the hub and the data center andbetween the call center and the data center.**	V1. Flawed / inadequate design, inappropriate / incomplete implementation.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment		Medium Exploitation of vulnerabilities present in devices may allow for breach of confidentiality or medical data integrity (e.g. Virus, worm, targeted attack) In addition a lack of proper security controls may allow an intervening party to eavesdrop, insert, alter or delete data which is in transit. This can occur at any point in the path of data and the remote access nature of

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
					the service offers even more opportunities for these types of breaches. In addition close proximity wireless communications also offer such opportunities since the communicating devices often do not have strong security mechanisms and the low strength of the radio signals provide a false sense of security.
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
		V7. Multiple actors (patient, SPs, call center etc.) have access to	A8. Data collector / Home Hub A10. Data centre and call centre		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		data	A16. RPM Service / Disease Management Program A15.Hospital IT System		
		V9. Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V10. Lack of or inadequate identification & authentication controls	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V11. Unsecured interfaces, non-existing or weak access control.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V13. Unmanaged IT Equipment	A7. Health monitoring devices		

Analysing the scenario						
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*						
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**		**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.	A8. Data collector / Home Hub A9. Personal IT equipment			
		V14. Unencrypted Data Storage	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System			
		V15. Wireless networks security shortcomings 1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment			
T5.	**Compromising the**	V5. Devices and equipment used in	A6. Health card			Medium to high

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
	availability of the service through various attack vectors. **e.g. D.o.S. Attack.**	unprotected/outdoor environments.	A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
		V9. Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V13. Unmanaged IT Equipment 1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.			
		V15. Wireless networks security	A7. Health monitoring devices		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		shortcomings 1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A8. Data collector / Home Hub A9. Personal IT equipment		
T6.	**Measurement devices or hub overloaded with too many measurements.**	V1. Flawed / inadequate design, inappropriate / incomplete implementation.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Medium to high before applying standard comm. security tech. such as BT security Depends on the importance of the measurements (probably low). It could be due to: • too many connected devices • patient takes too many measurements before it is possible that these are

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
					transmitted. Patient could be in an emergency state, requiring many measurements or he is panicked.
		V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V8. Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub		
T7.	**Monitoring devices are damaged in everyday mishaps, e.g. by user's carelessness (garment falls from stand,**	V2. Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management		Given the shift to the patient in terms of being responsible for a certain amount of equipment, it can be reasonably expected that

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
	accumulated dirt by coffee spills, etc).		Program		incidences of damage or wear and tear will occur. For example, garments may be put into the washing machine whilst forgetting to remove devices. e.g. Patient is exposed to sudden heavy rainfall while in an outdoor activity, where the equipment gets wet.
		V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub		
		Low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
T8.	**Natural threats (fire, flood, earthquake etc.)**	V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
T9.	**Malfunction/breakdown of systems affecting the**	V1. Flawed / inadequate design, inappropriate / incomplete	A6. Health card A7. Health monitoring devices		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
	delivery of the RPM service	implementation.	A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		
		V8. Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub		
T10.	**Patient's special garment or IT equipment is lost or stolen.**	V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
T11.	**non-expert usage of technological devices**	V2. Lack of usability/convenience and increased complexity or error proneness of the system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		
		V12. Low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
T12.	**Unauthorized use of measurement devices**	V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		Medium to high Depending on the measurement type and valueswrong measurements can be introduced which could lead to incorrect treatment which means a

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
					higher risk for the patient (which could lead to serious injuries).
		V8. Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub		
		V10. Lack of or inadequate identification & authentication controls	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V11. Lack of or inadequate logical access control	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
T13.	**Unauthorized access, modification and/or deletion of patient data,**	V1. Flawed / inadequate design, inappropriate / incomplete implementation.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub		Low to medium; Probably the patient trusts most of these people.

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
	along the chain of data collection and processing, by unauthorised individuals		A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Most likely a family member assisting the patient accesses the health data on the hub; or service staff engaged in repairing the hub, etc.
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
		V7. Multiple actors (patient, SPs, call center, etc) have access to data	A8. Data collector / Home Hub A10. Data centre and call centre A16. RPM Service / Disease Management Program A15.Hospital IT System		
		V9. Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre		

Analysing the scenario						
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*						
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**		**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
			A17. Hospital IT System			
		V10. Lack of or inadequate identification & authentication controls	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System			
		V11. Lack of or inadequate logical access control	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System			
		V13. Unmanaged IT Equipment 1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment			

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		V14. Unencrypted Data Storage	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V15. Wireless networks security shortcomings 1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment		
T14.	**Unauthorized access, modification and/or deletion of patient data, along the chain of data collection and processing, by authorised individuals**	V1. Flawed / inadequate design, inappropriate / incomplete implementation.	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Medium

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V5. Devices and equipment used in unprotected/outdoor environments.	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment		
		V7. Multiple actors (patient, SPs, call center, etc) have access to data	A8. Data collector / Home Hub A10. Data centre and call centre A16. RPM Service / Disease Management Program A15.Hospital IT System		
		V9. Devices communicate over unprotected or publicly accessible channels	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V10. Lack of or inadequate	A7. Health monitoring devices		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		identification & authentication controls	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V11. Lack of or inadequate logical access control	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V13. Unmanaged IT Equipment 1. Susceptible to OS and application vulnerabilities. 2. Susceptible to malware 3. Susceptible to firmware substitution allowing, backdoors and key loggers, covert channels etc.	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment		
		V14. Unencrypted Data Storage	A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			A17. Hospital IT System		
		V15. Wireless networks security shortcomings 1. Wireless networks susceptible to interceptions 2. Weakness of security controls/protocols	A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment		
T15.	**Data surveillance (dataveillance) and profiling**	V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		High
		V7. Multiple actors (patient, SPs, call center, etc) have access to data	A8. Data collector / Home Hub A10. Data centre and call centre A16. RPM Service / Disease Management Program A15.Hospital IT System		
		V11. Lack of or inadequate logical access control	A7. Health monitoring devices A8. Data collector / Home Hub		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
			A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System		
		V12. Low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V16. Lack of common legislation / interpretation in EU member states.	A15. Medical Procedures and Operational Standards A3. National Healthcare System		
		V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System		
		V18. Informed Consent statement	A15. Medical Procedures and Operational		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		that the patient has to sign is too intrusive and inappropriate	Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data is accessed or where this occurs or by whom and why.	A11. ELECTRONIC HEALTH RECORD A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and which are linked / connected.	A10. Data centre and call centre A16. RPM Service / Disease Management Program A17. Hospital IT System		
T16.	**Collected data can be inappropriately used for research or other**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub		Low, Secondary use of data for purposes other than those

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
	purposes different than those they were initially intended for, without notification to the data owner or the person concerned.		A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		directly linked to healthcare (delivery) versus 'mere' profiling…
		V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V16. Lack of common legislation / interpretation in EU member states.	A15. Medical Procedures and Operational Standards A3. National Healthcare System		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data is accessed or where this occurs or by whom and why.	A11. Electronic Health Record A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and which are linked / connected.	A10. Data centre and call centre A16. RPM Service / Disease Management Program A17. Hospital IT System		
T17.	**Misinterpretation of data by patient**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Medium to High, Depending on the context and nature of the data being misinterpreted by the patient as well as the potential controls in place to ensure effective data reporting by patients this threat could range from rendering the management ineffective to possibly inducing a life threatening emergency.
		V3. Critical parts of the	A15. Medical Procedures and Operational		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
		monitoring/ treatment process are becoming the responsibility of the patient.	Standards A16. RPM Service / Disease Management Program		
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V22. Complexity of medical data	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data		
T18.	**Misinterpretation of data by medical staff**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management		Low to High, Given that remote monitoring implies situations where medical professionals must rely on data not directly observed, there are risks involved in the misinterpretation of this

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			Program A17. Hospital IT System		data which could range from management efficiencies to those inducing life threatening emergencies.
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V22. Complexity of medical data	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data		
T19.	**Human error in cases of emergency**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards		High - As medical professionals need to rely on sensors providing remote data that cannot be directly observed there is the potential for human error in

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
			A16. RPM Service / Disease Management Program A17. Hospital IT System		cases of emergency. This could range from incorrect procedures in the handling of emergency related data to delays in response time, due to technical issues as well as human delays.
		V2. Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		
		V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V20. Different level of treatment in different countries.	A1. Health / Life A3. National Healthcare System		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			A5. Mobility of people		
		V22. Complexity of medical data	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data		
T20.	**Non Compliance with data protection legislation**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Low, Significant data protection legislation exists at EU level and within respective member states. However there are potential complications, for example if patients travel between EU member states, or travel outside of the EU with how is data transfer between jurisdictions and areas handled. How is primary data protection compliance maintained in such

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
					circumstances?
		V2. Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		
		V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment 4. pertinent regulations and legislation (e.g. data protection)	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V16. Lack of common legislation /	A15. Medical Procedures and Operational		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		interpretation in EU member states.	Standards A3. National Healthcare System		
		V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data is accessed or where this occurs or by whom and why.	A11. ELECTRONIC HEALTH RECORD A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management		

Analysing the scenario					
D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*					
No.	**Threat Description**	**Exploited Vulnerability*[1]**	**Affected Asset(s)**	**Threat agent** *(see table below)*	**Threat Assessment** *[High, Medium, Low with some explanation about selected level]*
			Program		
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and which are linked / connected (data linkability).	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A16. RPM Service / Disease Management Program A17. Hospital IT System Data		
T21.	**Inadequate provision or unavailability of medical service.**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		Low to High, There are substantial differences in the provision of health care between member states. There are as of yet no harmonised EU policies in relation to mandating health care provision in member states, other than OMC measures. Given the

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
					potential costs associated with the system described this could be a fundamental challenge to the system benefiting European patients in a diverse range of health care provision contexts.
		V2. Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		
		V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		V6. Lack of interoperability between devices and/or technologies and/or systems	A6. Health card A7. Health monitoring devices A10. Data centre and call centre A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V16. Lack of common legislation / interpretation in EU member states.	A15. Medical Procedures and Operational Standards A3. National Healthcare System		
		V20. Different level of treatment in different countries.	A1. Health / Life A3. National Healthcare System A5. Mobility of people		
T22.	**Low acceptance of RPM service and/or health care system by participating actors**	V1. Flawed / inadequate design, inappropriate / incomplete implementation	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A15. Medical Procedures and Operational		Medium, It cannot be assumed that medical professionals as well as patients will be universally accepting in terms of using

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			Standards A16. RPM Service / Disease Management Program A17. Hospital IT System		the proposed technological system outlined in the scenario
		V2. Lack of usability/convenience and increased complexity or error prone system/service/devices/equipment	A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A16. RPM Service / Disease Management Program		
		V3. Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient.	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V4. Excessive dependency on external infrastructures (e.g. ePrescription, PKI infrastructure for secure communications, digital authorisation, eID, etc.)	A13. Electronic Prescription A16. RPM Service / Disease Management Program A3. National Healthcare System		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		V6. Lack of interoperability between devices and/or technologies and/or systems	A6. Health card A7. Health monitoring devices A10. Data centre and call centre A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V8. Reduced device functionality or low quality / inadequate performance	A7. Health monitoring devices A8. Data collector / Home Hub		
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment 4. pertinent regulations and legislation (e.g. data protection)	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V17. Non-applicability of patient consent in the technical environment	A10. Data centre and call centre A15. Medical Procedures and Operational Standards		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			A16. RPM Service / Disease Management Program A17. Hospital IT System A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data is accessed or where this occurs or by whom and why.	A11. ELECTRONIC HEALTH RECORD A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V20. Different level of treatment in different countries.	A1. Health / Life A3. National Healthcare System A5. Mobility of people		
		V21. Huge amounts of data	A10. Data centre and call centre		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		(personal and medical) collected and stored in databases easily accessible and which are linked / connected (data linkability).	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A16. RPM Service / Disease Management Program A17. Hospital IT System Data		
		V22. Complexity of medical data	A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data		
T23.	**Populist political agenda**	V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment 4. pertinent regulations and legislation (e.g. data protection)	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		Medium. In a democracy with an effective free press one would expect resilience against this, however we cannot take this resilience for granted.
		V16. Lack of common legislation /	A15. Medical Procedures and Operational		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
		interpretation in EU member states.	Standards A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System A4. Human rights and social values		
		V19. Lack of data traceability. The Patient cannot be aware when his data is accessed or where this occurs or by whom and why.	A11. ELECTRONIC HEALTH RECORD A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program		
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and which are linked / connected (data linkability).	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A16. RPM Service / Disease Management Program		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			A17. Hospital IT System		
T24.	**Profit seeking attitude**	V7. Multiple actors (patient, SPs, call center, etc) have access to data	A8. Data collector / Home Hub A10. Data centre and call centre A16. RPM Service / Disease Management Program A15.Hospital IT System		High. The incentives of the present socio-economic infrastructure direct efforts towards putting as much monitoring devices and subsequent health plans and/or treatments into the market as possible.
		V12. Lack of or low awareness of 1. Information security 2. IT 3. RPM system and equipment 4. pertinent regulations and legislation (e.g. data protection)	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A3. National Healthcare System		
		V18. Informed Consent statement that the patient has to sign is too intrusive and inappropriate	A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management		

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
			Program A3. National Healthcare System A4. Human rights and social values		
		V21. Huge amounts of data (personal and medical) collected and stored in databases easily accessible and which are linked / connected (data linkability).	A10. Data centre and call centre A11. Electronic Health Record A12. Health Journal A13. Electronic Prescription A14. Public health research data A16. RPM Service / Disease Management Program A17. Hospital IT System		

Threat agent [further information] *[2]

No.	Threat agent (TA) [e.g. malicious user]	TA Motivation	TA Capacity (knowledge etc.)
TA1.	**Populist political party (or a populist politician)**	**Having control over a population, finding a scapegoat**	Depends on how access to data is organised and regulated
TA2.	**Populist media**	**Using the findings of profiling technologies to stigmatise certain groups**	Depends on how access to data is organised and regulated
TA3.	**Pharmaceutical industry**	**Creating or maintaining a competitive advantage**	Depends on how access to data is organised and regulated
TA4.	**Insurance company**	**Reducing risk, adequate price discrimination**	Depends on how access to data is organised and regulated

Analysing the scenario

D. Threats *[perceived threats that could exploit the identified vulnerabilities of the assets]*

No.	Threat Description	Exploited Vulnerability*[1]	Affected Asset(s)	Threat agent *(see table below)*	Threat Assessment *[High, Medium, Low with some explanation about selected level]*
TA5.	**Employers**	**Risk reduction**	Depends on how access to data is organised and regulated		
TA6.	**Attacker**	**Just to cause harm or earn money (valuable to insurance companies, employers, healthcare research, etc.), Curiosity**	Medium		
TA7.	**Family and friends**	**Curiosity, Personal benefit**	Low		
TA8.	**Service staff**	**By Error, Curiosity, Testing the device, money (valuable to insurance companies, employers, healthcare research, etc.)**	Medium to high		
TA9.	**Patient**	**By Error, Preventing increasing insurance premium, abuse of social security, Irritation or ignorance**	Lack of Knowledge, Low		
TA10	**Medical Professionals**	**Personal benefit, irritation or ignorance**	Lack of knowledge and expertise		
TA11	**Non-medical actors and organisations**	**Varied**	Varied (i.e. criminal investigations, insurance, fraud detection)		
	[1] Note that the same threat may exploit more than one vulnerability of the same or different assets. ***[2] In case the threat is of human origin; if it is an environmental threat (like earthquake, fire etc.), you do not need to fill this in.***				

Analysing the scenario

E. Impact *[estimation of impact of the identified threats; it is closely related to the asset value, so you need to consider that]*

No.	Impact	Description
Legal and Ethical		
I01	Be legally framed - being used as a scapegoat	Volatility of data may allow for alteration that leads to the incrimination of the wrong individual.
I02	Avoidance of insurance liabilities.	Insurance companies may claim that the health problem was a result of patient's choice and thus not covered by the insurance contract.
I03	Health professionals are not held liable for unprofessional judgement/behaviour.	In the presence of increased patient responsibility medical professionals can avoid liabilities in respect of unprofessional behaviour/judgement that may lead to patient's health damage.
Social and Political		
I04	Breach of trust relationship between the patients and most importantly damage of citizens' trust of to the healthcare system	
I05	Society rejects use of technology	Relates to social acceptance of the technologies
I06	Social discrimination based on health data	e.g. : Loss of employment opportunities, Insurance companies offering premiums for customers that belong to groups that exhibit fewer risks of becoming sick,
I07	Exclusion from insurance, health services or social security coverage	Availability of data implying patient has hazardous habits (e.g. smoking) or he is not compliant with his health plan Non-compliance by Ralph may jeopardize access to insurance (for life, for health, but also social security) etc. E.g. refusal of kidney transplants to patients who continue to drink, cancer treatments for those who continue to smoke. Or focus on 'outliers' (e.g. those whose health does not improve), allowing that 'adequate' measures have been undertook enforcing the tendency to focus on

Analysing the scenario		
E. Impact *[estimation of impact of the identified threats; it is closely related to the asset value, so you need to consider that]*		
		'relative risk reduction' instead of 'number needed to treat'.
Health		
I08	Loss of Life	
I09	Health Deterioration	
Financial / Economical		
I10	Patient claims for reparations	
I11	Increased costs for the patient	
Organisational / Technological		
I12	Inefficiency in Care Delivery	Supplying lower quality care to patients or failing to reach the envisioned/required patient treating capacity.
I13	Prolonged RPM service unavailability	

Analysing the scenario
F. Acceptable risk level *[estimation of levels of risk that are derived from the subject matter area and concern above assets, vulnerabilities and impacts. The risk level are classified via a scale from 1-10]*
Please refer to Annex II – EFR Pilot Risk Analysis Report.

Analysing the scenario

G. Assumptions *[any assumptions made during the analysis, i.e. identification of vulnerabilities, threats, impact etc.]*

1. It is assumed that indirectly or directly an amount of personal data is generated by the use of the system. This will ultimately depend on the particular national and potential EU context of health care provision. Perhaps the scenario needs to also set clearer specifications on the types and the limitations to the data which is collected. For example location may not be stored, but only used in cases of emergency.

2. It has been assumed that the scheme is a relatively new implementation. There are issues then as a result about public and medical awareness and acceptance of the technology along with issues related to knowledge about effective use of the system. These would as indicate need some consideration in terms of fleshing out the human dimension of interaction with the system.

3. It has been assumed (as does the scenario) that appropriate network infrastructures exist for the successful implementation of the system. However given the uneven state of network infrastructures across the EU there may be a case to be made that within some areas of the EU successful implementation of the system may be difficult even within the timeframe of two years. This may especially be true of new member states. What will however vary substantially without EU intervention is the maintenance and operational costs of the networks involved.

4. There is an assumption that enhancing the autonomy of patients, and a shift towards individualisation of medical care is a 'good' impact. This is a debatable point. Autonomy and individualisation may depend on an 'active citizen' approach to health care but this may have substantive implications if we consider the limitations due to inequalities and inequities in health care access between different groups and individuals across the Union in accessing health care in just and equal ways.

5. Access to the RPM service can be achieved by using the health card, but also by providing other means of identification (ID, Name and secret question or personal information)

Analysing the scenario
G. Assumptions *[any assumptions made during the analysis, i.e. identification of vulnerabilities, threats, impact etc.]*
6. Health card contains a small amount of data that are encrypted and not very sensitive. 7. Ralph's data is anonymised and used for public health research.

Glossary / Aid

Here are some definitions of the terms / concepts according to ISO/IEC 13335-1 (2004)[3] and the Glossary in ENISA Web-site[4] that you see are required to be filled in the table above and which will help you fill in the table.

Asset – Anything that has a value to the organisation (note: in our case not only the organisation...). These assets have value to the organization, which is normally expressed in terms of the impact on business operations from unauthorized disclosure, modification or repudiation of information, or unavailability or destruction of information or service.

Vulnerability - A weakness of an asset or group of assets that can be exploited by one or more threats. Refers to an aspect of a system that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance or attack. A vulnerability can exist in the absence of corresponding threats and in itself it does not cause harm; a vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Vulnerabilities arising from different sources need to be considered, for example, those intrinsic or extrinsic to the asset.

Threat – An activity or event the occurrence of which could have an undesirable impact; the circumstance or event has the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats may be of environmental or human origin and, in the latter case, may be either accidental or deliberate. Statistical data are available concerning many types of environmental threats. Such data may be obtained and used by an organization while assessing threats. Threats have characteristics that define their relationships with other security elements. These characteristics may include the following:

- motivation, e.g. financial gain, competitive advantage,
- frequency of occurrence,

---

[3] *ISO / IEC 13335-1 (2004) "Information technology - Security techniques - Management of information and communications technology security — Part 1:Concepts and models for information and communications technology security management"*

[4] *http://www.enisa.europa.eu/rmra/glossary.html*

- likelihood, and
- impact

Impact - The loss or degradation of a business value (money, reputation, trust etc.) or any other loss that could have been the consequence of a particular violation. Impact is the result of an information security incident, caused by a threat, which affects assets.
The impact could be the destruction of certain assets, damage to the ICT system, and compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Possible indirect impact includes financial losses, and the loss of market share or company image.

Glossary [*scenario specific*]

Call center - typically by nurses and other specialized health professionals it operates 24/7 and are allowed to contact the subscriber, their family physician and ambulance services in accordance to the alarm level. In the prospective scenario, the call center has access to biometrics and health profile of the subscriber.

Data center – Independent organization that manages the medical data on behalf of the hospital or the health plan ensuring security, privacy and resilience as a trusted third party.

Health journal: a personal health record linked to Ralf's health plan where he records his daily activities, and data from various medical devices are recorded
Health monitoring report: Based on the biodata

Health monitoring report: Based on the biodata collected from various devices and Ralfs own remarks a summary report is compiled on a daily/weekly/biweekly basis. Ralf's family doctor, reviews it during the medical-televisit, and possibly uses it as input to his own report.

Other information

[You may provide here other information you consider relevant and cannot be covered in the fields above, e.g. images etc.]

References

Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, adopted on 15 Feb 2007.

Carvel, John, "Four-year delay for NHS's new IT system", *The Guardian*, 16 May 2008.
http://www.guardian.co.uk/society/2008/may/16/nhs.health

Carvel, John, "Family doctors to shun national database of patients' records", *The Guardian*, 20 Nov 2007.
http://www.guardian.co.uk/society/2007/nov/20/nhs.health

European Commission, e-Health – making healthcare better for European citizens: An action plan for a European e-Health Area, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2004) 356 (final), Brussels, 30 Apr 2004.

European Commission Information Society and Media, ICT for Health and i2010: Transforming the European healthcare landscape: Towards a strategy for ICT for Health, Office for Official Publications of the European Communities, Luxembourg, 2006.

European Commission, DG Information Society and Media, Benchmarking ICT use among General Practitioners in Europe, Final Report, Bonn, April 2008.
http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm#NEW_Pilot_on_eHealth_indicators:_Benchmarking_ICT_use_among_General_Practitioners_in_Europe

European Commission, "eHealth initiatives to support medical assistance while travelling and living abroad", Press release, IP/08/1075, Brussels, 2 July 2008.
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1075&format=HTML&aged=0&language=EN&guiLanguage=nl

Gellman, Robert, "Health Privacy: The Way We Live Now", *Privacy Papers,* Free Congress Foundation, August 2002.
http://www.privacyrights.org/ar/gellman-med.htm

Levy, Steven, "Hazardous to Your Privacy? ", *Washington Post,* 27 Feb 2008.
http://www.washingtonpost.com/wp-dyn/content/article/2008/02/26/AR2008022602993.html

Lohr, Steve, "Warning on Storage of Health Records", *New York Times,* 17 April 2008.
http://www.nytimes.com/2008/04/17/business/17record.html?_r=1&oref=slogin

Lohr, Steve, "Google Offers Personal Health Records on the Web", *The New York Times,* 20 May 2008.
http://www.nytimes.com/2008/05/20/technology/20google.html?_r=1&ref=technology&oref=slogin.