‘Being diabetic in 2011’

Identifying emerging and future risks in remote health monitoring and treatment

ANNEX II – *The Risk Analysis Report*

Prepared by

logica management consulting

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.

About this report

This report has been prepared by *Guillaume Le Galiard*, *Adèle Adam* and *Hervé Ysnel* of **Logica Consulting**, as a result of the risk analysis performed for the ENISA EFR Pilot "Being diabetic in 2011" on remote health treatment and monitoring subject.

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

Contents

Risk assessment methodology

Introduction

This risk analysis is based on the EBIOS methodology. A risk is the consequence of a threat that exploited a vulnerability that exists on an asset. In EBIOS, risks are strongly related to threats and are linked with vulnerabilities and impacts, this relationship is represented in the schema below (see Figure 1). That is why the calculation of risk level takes into account these 3 parameters. This calculation is explained later in the document.

Figure 1 - Risk calculation

This document is divided in two main parts. In this first part, the risk assessment methodology will be presented. It consists mainly of explaining what parameters have been taken into account in evaluating the risk, why these have been chosen and where they originate from.

Evaluation of the probability

The evaluation of the probability that a risk occurs is a very important parameter in evaluating a risk. In this section, the way it is calculated will be explained. Two parameters are needed to evaluate the probability: the attack potential and the opportunity. In the two following sub-sections, more specific information is given concerning these latter parameters. The third subsection presents a scale for calculating the probability using the two previously cited parameters.

Attack potential

The attack potential is related to the threat level. For each threat, it has been determined that an attack potential can be rated from "Low" (1) to "High" (5) as it is summarized in Table 1.

Level (correspondence)	Description (ENISA)	Example (EBIOS)
1	Low	accidental and random
2	Low to Medium	
3	Medium	limited opportunities or resources

4	Medium to High	
5	High	high level of expertise, opportunity and resources

Table 1 - Attack Potential

In the study done by ENISA, threat agents were determined for each threat. Those threat agents had a capacity (called "TA capacity") rated by ENISA from "Low" to "High". This "TA Capacity" is the same parameter required in an EBIOS analysis as the attack potential. In order to make the calculation easier, it has been decided to associate numbers from 1 to 5 to represent ENISA's levels (see Table 1). To give a general idea of what each level can mean, some examples are given in the last column of the table above. These examples are taken from the Knowledge Base of the EBIOS software tool.

Opportunity

The Opportunity is related to the vulnerability level. A list of vulnerabilities corresponds to each threat. Each of the vulnerabilities has been rated by ENISA during the case study from "Low" to "High". To adapt this level to a calculation, numbers from 1 to 5 have been assigned to each level as can be seen in Table 2. The opportunity is expressed in the EBIOS knowledge database as ranging from "Totally improbable" to "certain" which is then mapped to each of the levels needed to calculate the vulnerabilities levels. In addition, in the database, the Knowledge/Means needed to exploit each of the vulnerabilities is given. This gives a better understanding of what an attacker needs to exploit vulnerabilities.

Description (ENISA)	Level (correspondence)	Opportunity (EBIOS)	Knowledge/Means (EBIOS)
Low	1	Totally improbable	Unfeasible
Low to Medium	2	Low probability	Needing very considerable means and/or a very high level of knowledge in the field concerned
Medium	3	Medium probability	Needing a certain level of expertise and/or specific equipment
Medium to High	4	High probability	Possible using standard means and/or basic knowledge
High	5	Certain	Possible for anyone

Table 2 - Scale of opportunities

A risk is composed of several vulnerabilities. The opportunity must be a representative value of all of those vulnerabilities levels. That is why, to obtain the opportunity, the maximum of the levels has been taken.

Probability scale

Now that the origin of the attack potential and the opportunity have been seen, it must be explained how they are related to each other in order to give the probability. The following grid (see Figure 2) depicts this relationship. The numbers entered in the grid depend on the context of the study. The priority can be given to the opportunity or the attack potential or both.

To illustrate this, we can consider a risk with an opportunity of 4 and an attack potential of 5, the probability for this risk to occur would be at the intersection of these two results, that is to say 3.

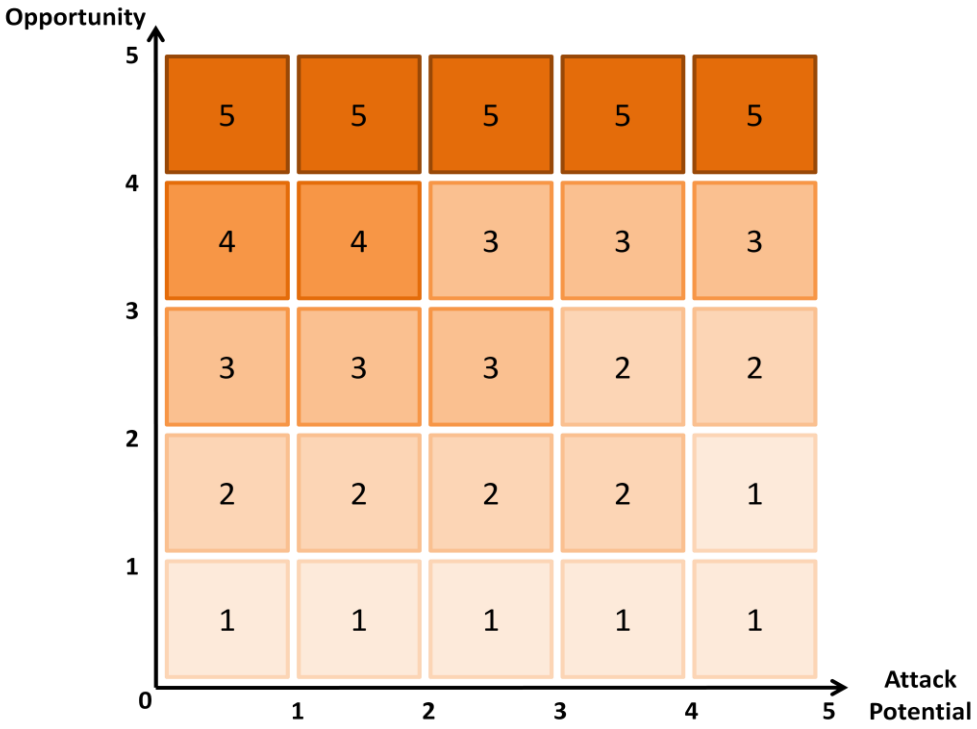


Figure 2 - Probability Scale

Calculation of the risk level

The seriousness of a risk is evaluated in taking into account two parameters: the probability and the impact. This step is presented in the second subsection.

Before that, each of the parameters should be detailed. However, it needs to be remembered that the way in which the probability can be obtained has just been explained in the previous paragraph (using the opportunity and the attack potential). That is why in the following subsection, only the impact assessment will be tackled.

In the last subsection, a last parameter known as the risk tolerance will be explained and how it will be used in the study.

Impact assessment

During the study it has been decided that the impacts would be divided into five categories which are Health, Social/Political, Legal/Ethical, Organisational/Technological and Financial/Technological. However, those categories are quite large and more specific impacts have been defined by ENISA in each of the categories (noted as I01, I02, etc.).

On the other hand, the impacts also needed to be evaluated according to levels. Those have been defined both with numbers and level titles from "Very Low" (1) to "Very High" (5).

In order to make the assessment clear, each of the sub-impacts (I01, I02, etc.) has been split according to the different level set. The result is presented in the grid below (Table 3).

Impact Value		Health	Social and Political	Legal and Ethical	Organisational / Technological	Financial / Economical
1	**Very Low**					I10.1: Patient claims for reparations. (less than 1 500 Euros).
2	**Low**					I10.2: Patient claims for reparations (less than de 15 000 Euros).
3	**Medium**		I04: Breach of trust relationship between the healthcare system and the patient.			I10.3: Patient claims for reparations (less than 150.000 Euros).
4	**High**	I09: Health deterioration.	I06: Social discrimination based on health data.	I01: Be legally framed - being used as a scapegoat.	I12: Inefficiency in care delivery.	I10.4: Patient claims for reparations (less than de 1 500 000 Euros).
			I05: Society rejects use of technology, and the system becomes useless.			I11: Increased costs for patient.

5	**Very High**	I08: Loss of Life.		I02: Avoidance of insurance liabilities.	I13: Prolonged RPM service unavailability.	I.10.5: Patient claims for reparations (less than 15 000 000 Euros).
			I07: Exclusion from insurance, health services or social security coverage.	I03: Health professionals are not held liable for unprofessional judgement/behaviour		

Table 3 - Impact Scale

As a risk can generate several impacts, the maximum impact level is considered because it represents the worst consequence that could be generated by the risk involved.

Risk level

The assessment of the risk level is expressed using the two parameters: probability and impact. The probability is the chance that the considered risk will occur while the impact is the effects which this risk could generate. The following grid (see Figure 3) depicts the expression of the risk level depending on these two parameters.

For instance, if the probability of a risk to happen is 3 and the impact this risk could generate are 4, we can produce the risk level which is the intersection of the two parameters: here the risk level would be 4.

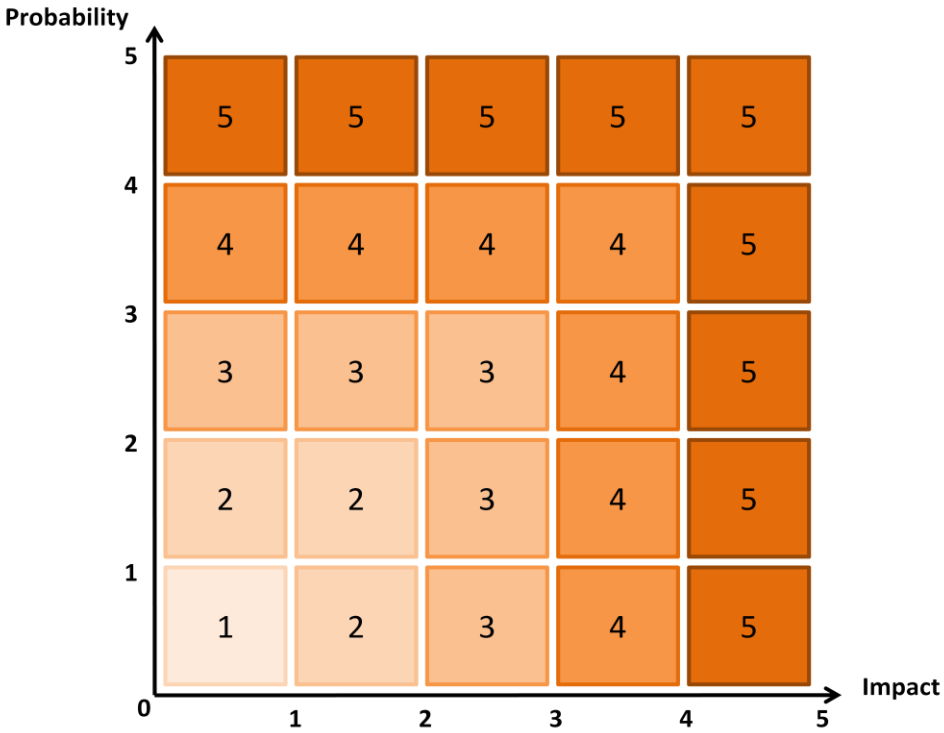


Figure 3 - Risk Scale

Risk tolerance

All the risks have a chance to occur but depending on the assets they are concerned with, they are more or less likely to be tolerated by the assets owner (or the actor or organisation responsible for this system). The assets have been rated by ENISA on a scale that ranges from "1" to "10", "1" being an asset of small value and "10" being an essential asset. From this scale, the risk tolerance can be determined.

On the one hand, the assets owner is likely to accept more easily a risk occurring on a small value asset. Thus, the tolerance would be high for this risk. On the other hand, a risk that could imply a very high value asset would be nearly inconceivable, which is why the

tolerance would be low. This relationship between the value of an asset and the tolerance of a risk is shown in Table 4.

Asset value	Risk Tolerance
1-4	High
5-7	Medium
8-9	Low
10	Very Low

Table 4 - Relation between Asset value and Risk Tolerance

Security Needs Scale

The following grid gives the levels of security needs for the three criteria: Confidentiality, Availability, and Integrity.
As it has not been taken into account in the study, we did not use CIA to evaluate the needs of the assets and as a consequence the impacts of the risks. But this data can be used later in the study.

	Availability	Confidentiality	Integrity
1	No availability need	No confidentiality need (Public)	No integrity need
		The data is public (no restriction)	
2	Long term	Restricted	Low Integrity need
	The essential element may be unavailable for more than a week, but must not be definitively lost.	Only authorized people (IT people, data centre people, hospital people, doctor, and patient) can access the data.	The essential data is controlled automatically.
3	Medium term	Confidential (Internal)	
	The essential element must be available in less than a week.	Only authorized medical staff and patient can access the data.	
4	Short term	Confidential (High)	High Integrity need
	The essential element must be available during the day.	Only the patient's doctor and the patient are authorized to consult the data (medical privacy)	The essential data is controlled automatically and measurement coherence is performed.
5	Very short term	Confidential (very high)	Very High Integrity need

	Availability	Confidentiality	Integrity
	The essential element must be available in real time.	Only the patient is able to consult the data. (secret)	The essential data is controlled and verified by the call centre/doctor. The data must be as accurate as possible.

Table 5 - Security Criteria

Risk analysis

Introduction

In this second part, the results of the risk analysis itself are presented. For each risk that has been determined during the study, a table has been produced to represent it. A blank table is pasted below to give an example of what kind of information will be given for each risk. At the end of this part, a classification of the risks given by risk levels is given.

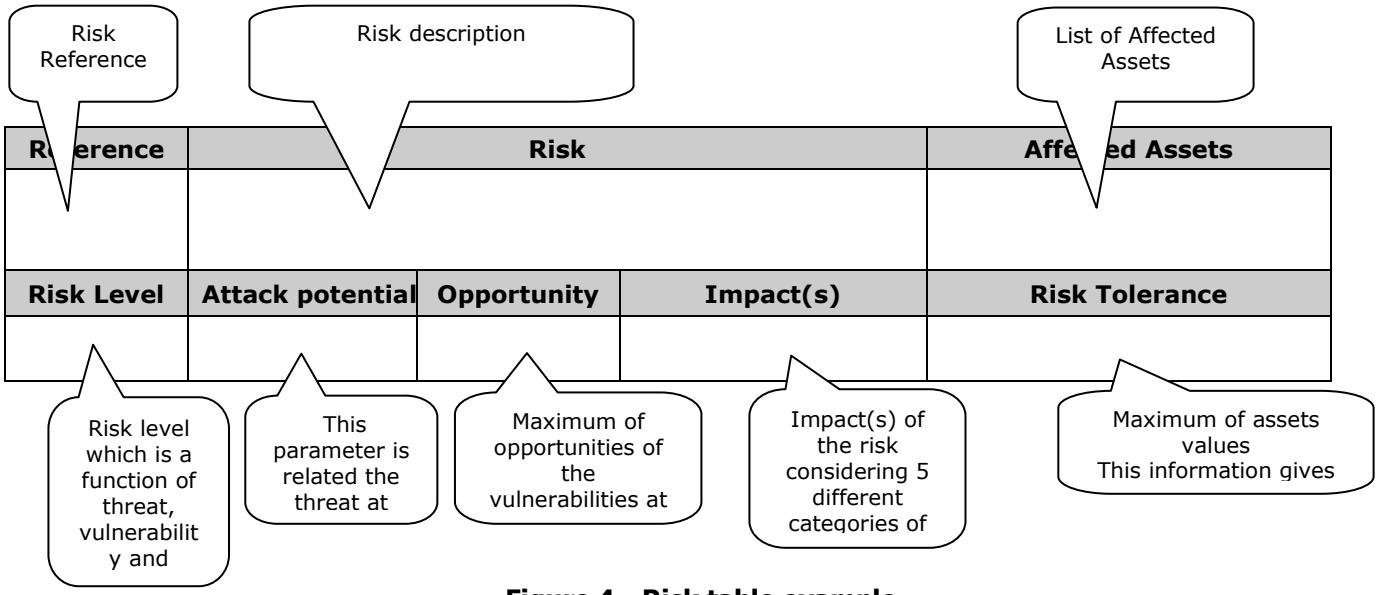


Figure 4 - Risk table example

Assumptions:

- Considering the complexity of the study and the important numbers of assets, we decided to describe a risk as starting from a threat, analysing the exploited vulnerabilities and focusing on the affected assets. This is the EBIOS approach as well and if we would have started from the assets we would have repeated the same risks several times.
- For the risk tolerance, we made the assumption of keeping the maximum value of the affected assets in order to retain all of the information from the study case.
- For the attack potential, the threat agent's capacity has been used. When several agents could provoke a risk, the maximum of the capacity has been chosen representing the most skilled agent.
- For the level of opportunity, we decided to keep the maximum because a threat just has to exploit the weakest vulnerability to affect the assets.
- For the impact level, we made the assumption that the general impact is equal to the level of the worst impact.

The following scale of colour will be used in the tables to represent the level of risk:

Low	Low to Medium	Medium	Medium to High	High
1	2	3	4	5

Figure 5 - Colour scale

Concrete example

To have a clearer view of how the calculus is made, this section will aim at showing step by step how the risk table has been filled in. The first risk will be taken as an example for this section.

First Step: Formulating the risks

For each threat, a risk has been produced. That is why the **Reference** number of the risk corresponds to the number of the threat. Here it is R01.

In the **Risk** box, three pieces of information can be found:

- The vulnerabilities that can be exploited (here v2, v3, v4, v12)
- A risk title coming from the threat it relates to
- The security criteria concerned by this risk (here confidentiality, integrity and availability)

The result of this step is the filling of the two following boxes:

Reference	Risk			Affected Assets
R01	The system might lack usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient might not follow the instructions to do with equipment use, treatment and medication.** That might affect the confidentiality, the integrity and the availability of the assets. The risk could lead to several impacts listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**

Second Step: The assets

The list of **affected assets** concerned has been copied from ENISA's study. Here the assets are those corresponding to the first threat. Into brackets, the asset value defined by ENISA has been reported.

We can see that the most important assets are those having a higher value, here 10. To determine the **risk tolerance** let's use Table 4. The excerpt of the table which is relevant for us is:

Asset value	Risk Tolerance
10	Very Low

Those results are added to our risk table below.

Reference	Risk			Affected Assets
R01	The system might lack usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient might not follow the instructions to do with equipment use, treatment and medication.** That might affect the confidentiality, the integrity and the availability of the assets. The risk could lead to several impacts listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
				Very Low (10)

Third step: calculating the probability

The attack potential

The threat agent of "T1. Patient does not follow the instructions to do with equipment use, treatment, medication" is "TA9. The patient". The patient's capacity has been defined by ENISA as "Lack of Knowledge, Low". As a result, the row considered in the attack potential table is:

Level	Description	Example
1	Low	accidental and random

The opportunity

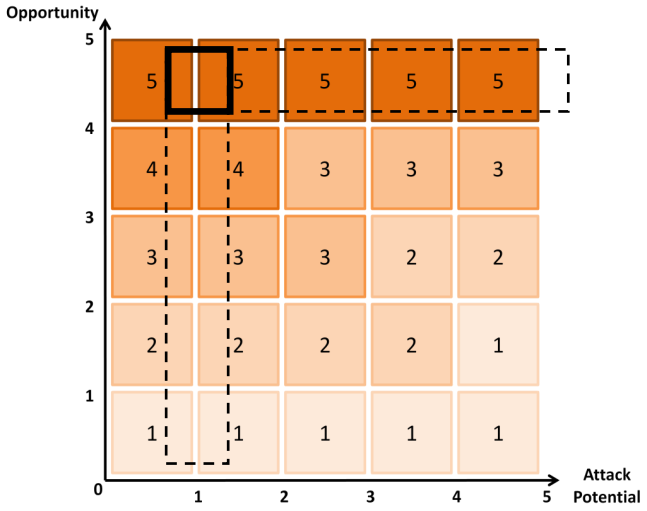
Here are the vulnerabilities related to this risk and their level as assessed by ENISA:

Number	Title	ENISA's assessment	Corresponding level
V2	"Lack of usability/convenience and increased complexity or error prone system / service / devices / equipment"	Medium to high	4
V3	"Critical parts of the monitoring/ treatment process are becoming the responsibility of the patient"	High	5
V4	"Excessive dependency on external infrastructures"	Medium	3
V12	"Low awareness of: 1.Information security, 2. IT, 3. RPM system and equipment"	High	5

The opportunity corresponds to the highest value of the vulnerabilities' level: here it is 5.

The probability

To obtain the probability, let us use the following grid. It has just been seen that the opportunity is 5 and the attack potential 1. The intersection between those two values is 5 has shown below.



Now we can fill in:

Reference	Risk	Affected Assets
R01	The system might lack usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient**	A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription

	might not follow the instructions to do with equipment use, treatment and medication. That might affect the confidentiality, the integrity and the availability of the assets. Risk that could lead to several impacts listed below.			A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potentia**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
	1	5		Very Low (10)

Fourth step: the impacts

The grid of impacts as well as their levels has been defined by ENISA (see Table 3). Then, a choice as been made, depending on which impact, the risk was likely to generate. For this first risk, the following impacts could be generated:

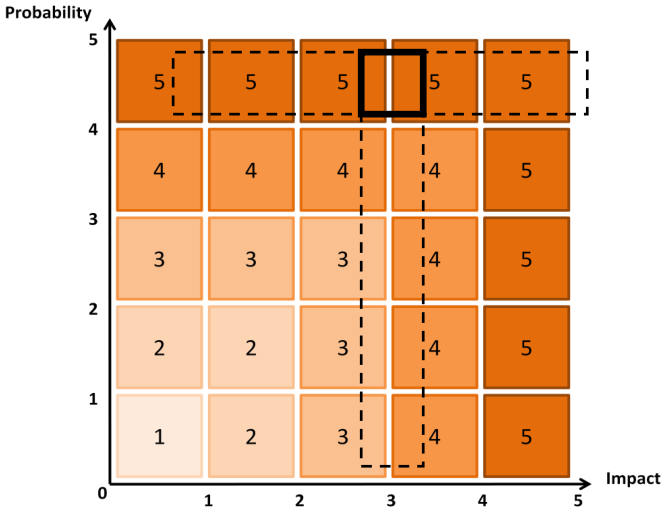
- Social/Political (I04): level 3
- Financial/Economical (I10): level 3
- Organisational/Technological (I12) : level 2

For the "risk level" calculus, we made the assumption that the maximum level of impact would represent the global impact of the risk. For instance, here the general impact is "medium".

Reference	**Risk**			**Affected Assets**
R01	The system might lack usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient might not follow the instructions to do with equipment use, treatment and medication.** That might affect the confidentiality, the integrity and the availability of the assets. Risk that could lead to several impacts listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
	1	5	- Social (I 04) = **3** - Financial (I 10) = **3** - Organizational (I 12) = 2	Very Low (10)

Final step: the risk level

We have a global impact level of 3 and a probability of 5. The intersection between those two rows gives us a risk level of 5. This gives us the final result in the risk table below.



Reference	Risk			Affected Assets
R01	The system might lack of usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient might not follow the instructions to do with equipment use, treatment and medication.** That might affect the confidentiality, the integrity and the availability of the assets. Risk that could lead to several impacts listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Social (I 04) = 3 - Financial (I 10) = 3 - Organizational (I 12) = 2	Very Low (10)

Presentation of risks

Reference	Risk			Affected Assets
R01	The system might lack of usability/convenience (v2) and the patient may have a low awareness of the system (v12). In addition, the patient's treatment becomes his responsibility (v3) and depends excessively on external infrastructure (v4). For those reasons, **there is a risk that the patient might not follow the instructions to do with equipment use, treatment and medication.** That might affect the confidentiality, the integrity and the availability of the assets. Risk that could lead to several impacts listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Social (I 04) = 3 - Financial (I 10) = 3 - Organizational (I 12) = 4	Very Low (10)

Reference	Risk			Affected Assets
R02	The data collected about the patient are numerous (v21) and it will be difficult for the latter to know when, why and by who the data is accessed (v19). Even if consent form are to be signed by the patient they could be intrusive (v18) or difficult to apply (v17). In addition, problems could exist in the system's implementation (v1) and the patient could have a low awareness of it or IT in general (v12). **For those reasons, there is a risk that the system is not compliant with informed consent legislation** which could lead to a breach of confidentiality regarding the assets considered. This could lead to the following impacts.			A3. National Healthcare System A4. Human rights and social values A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A11. Electronic Health Record A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Legal (I 03) = 5 - Social (I 04) = 3 - Financial (I 10) = 3	Very Low (10)

Reference	Risk			Affected Assets
R03	**A risk to compromise one's credentials could happen** due to the possible use of the equipment in unprotected environments (v5) and unprotected channels of communication (v9 and v15). In addition if the system does not possess an adequate means of authenticating the user (v10), the risk is higher. The lack of knowledge (v12) and of management (v13) in/of an IT system just as flaws in the system (v1) could also heighten the risk. The three criteria confidentiality, integrity and availability could be impacted on. The impacts that might be generated are listed below.			A3. National Healthcare System A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	3	5	-Organisational (I 13) = 5 -Social (I 04) = 3 -Financial (I 10) = 2	Very Low (10)

Reference	Risk			Affected Assets
R04	With such a system, it is important to consider **the risk that the confidentiality or the integrity of the data processed could be breached.** Indeed, the possibility of eavesdropping on communications (v5, v7, v9, and v15), a lack of protection (v14, v10, v11) and possible problems with the system (v1, v13) could have the following impacts.			A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Health (I 09) = 4 - Financial (I 10) = 3	Very Low (10)

Reference	Risk			Affected Assets
R05	**The availability of the service could be compromised** due to the use of the devices in unprotected environments (v5), via unprotected communication channels (v9, v15) and it might not be correctly managed (v13). This risk could represent a breach of confidentiality and of the availability of the assets, and to certain extent of integrity as well, which could lead to the impacts below.			A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**

5	3	4	- Organisational (I13) = 5 - Health (I 09) = 4	Very Low (10)

Reference	Risk			Affected Assets
R06	If the system is flawed (v1), if it depends on too many external infrastructures (v4) and if the devices are of low quality (v8), **there is a risk that the devices or hub could be overloaded.** As a consequence, the availability of the assets on the right may not be guaranteed.			A3. National Healthcare System A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	-Social (I 04) = 3 -Organizational (I12) = 4	Very Low (10)

Reference	Risk			Affected Assets
R07	**There is a risk of damaging the equipment** either because it is not convenient (v2), it is used in an unprotected/outdoor environment (v5) or because the users have a low awareness of the system and IT in general (v12). A result could be a reduction in the availability of the assets as well as the impacts below.			A3. National Healthcare System 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
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Financial (I 11) = 4 - Organizational (I13) = 5	Very Low (10)

Reference	Risk	Affected Assets
R08	**Natural threats could damage the system** due to its use in unprotected and/or outdoor environments (v5). Moreover, due to the fact that the system depends on numerous infrastructures (v4), these damages can happen at numerous points. This risk could lead to several impacts listed below. Regarding this risk, both the integrity and the availability of the assets could be breached.	A3. National Healthcare System A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A13. Electronic Prescription A16. RPM Service / Disease Management Program

Risk Level	Attack potential	Opportunity	Impact(s)	Risk Tolerance
5	1	3	- Financial (I 11) = 4 - Organizational (I13) = 5	Very Low (10)

Reference	Risk			Affected Assets
R09	The possible flaws in the system (v1) as well as the possible low quality and performance of the devices used (v8) could be responsible for **a risk of malfunction and breakdown of the system.** As a result the following impacts could happen as well as a reduction of the availability of the assets.			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
Risk Level	**Attack potenti**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Organizational (I13) = 5 - Financial (I 10) = 4 - Health (I09) = 4	Very Low (10)

Reference	Risk			Affected Assets
R10	**There is a risk that the patient's garment and/or IT equipment could be stolen** due to the fact that the system is used in unprotected and outdoor environments (v5) and due to the system being under the responsibility of the patient (v3). This could impact on the confidentiality and the availability of considered assets.			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
Risk Level	**Attack potentia**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	3	5	- Health (I 09) = 4 - Financial (I 11) = 4	Very Low (10)

Reference	Risk			Affected Assets
R11	**There is a risk the devices might be used unprofessionally**. Firstly because the user can have a low awareness of the system and more generally IT (v12) and secondly because the system is not always convenient (v2). The assets' confidentiality, integrity and availability could be impacted on.			A3. National Healthcare System 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
Risk Level	**Attack potentia**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Legal (I03) = 5 - Social (I07) = 5 - Financial (I 10) = 1	Very Low (10)

Reference	Risk			Affected Assets
R12	**There is a risk that the measurement devices could be used by unauthorized people** due to a lack of protection (v5, v10, v11) and to the possibility that the devices perform poorly (v8). The three security criteria concerned: confidentiality, integrity and availability may all be impacted on. The following impacts are the result when such a risk happens.			A6. Health card A7. Health monitoring devices, A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A17. Hospital IT System
Risk Level	**Attack potentia**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
4	3	4	- Technological (I 12) = 4 - Health (I 09) = 4	Very Low (10)

Reference	Risk			Affected Assets
R13	Due to flaws in the system (v1, v13), lack of controls (v10, v11, v7) and a low protection of the system (v5, v9, v14, v15) **a risk that unauthorized individuals might gain access, modify and/or delete the patient's data could exist.** Confidentiality, integrity and availability could be impacted on. The four impacts that follow could be a result of the appearance of this risk.			A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potentia**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Financial (I 10) = 2 - Technological (I 12) = 4 - Health (I 09) = 4 - Social (I 04) = 3	Very Low (10)

Reference	Risk	Affected Assets
R14	If there is a risk that unauthorized individuals gain unauthorized access to modify and/or delete the patient's data, another similar risk should be considered: this is **the fact that the modification and/or deletion of patient data can be performed by authorized individuals.** In addition to the vulnerabilities expressed by the previous risk, the responsibility of the patients is added here (v3). All the three security criteria are concerned: confidentiality, integrity and availability. The	A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A15. Medical Procedures and Operational Standards A16. RPM Service / Disease

	four impacts that follow could be a result of the appearance of this risk.			Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Financial (I 10) = 2 - Technological (I 12) = 4 - Health (I 09) = 4 - Legal (I 03) = 5	Very Low (10)

Reference	**Risk**			**Affected Assets**
R15	**There can be a risk of data surveillance and profiling** when there is a lack of control over the data or the system (v11, v7, v19, v21), particularly where it can be seen that the system depends a lot on external infrastructures (v4), when there can be numerous problems with consent (v16, v17, v18) and when the users have a low awareness of IT (v12). Confidentiality, integrity and availability could be impacted. The different impacts generated by such a risk are detailed below.			A3. National Healthcare System A4. Human rights and social values A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A11. Electronic Health Record A13. Electronic Prescription A15.Hospital IT System A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Financial (I 10) = 3 - Social (I 06) = 4	Very Low (10)

Reference	**Risk**	**Affected Assets**
R16	Due to the huge amount of data collected (v21) where consent or legislation is not always followed in its collection or processing (v 16, v17, v18, v19) and due to the fact that the excessively dependent to external infrastructures (v4) where the system can have flaws (v1) or can be used by users that lack awareness (v12), the following risk could appear. **The collected data could be inappropriately used for research or other purposes different than those they were initially intended for.** The confidentiality, integrity and availability of the assets might not be guaranteed. Such a risk could cause the impacts listed below.	A3. National Healthcare System A4. Human rights and social values A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A11. Electronic Health Record A13. Electronic Prescription A15. Medical Procedures and

				Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack Potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	3	5	- Financial (I 10) = 3 - Legal (I 02) = 5 - Social (I 04) = 3	Very Low (10)

Reference	Risk			Affected Assets
R17	**There is a risk that the patient might misinterpret the data** either because of flaws in the system (v1), the patient's low awareness of the system and IT (v12) and the complexity of medical data (v22). This risk is all the more important in that critical parts of the patient's monitoring and treatment are becoming his responsibility (v3). The confidentiality, integrity and availability of the assets might not be respected. This risk could generate the following impacts.			A3. National Healthcare System 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 A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Financial (I 10) = 2 - Health (I 08) = 4	Very Low (10)

Reference	Risk			Affected Assets
R18	If the patient misinterprets his/her data, there is also **the risk that the misinterpretation comes from a mistake made by medical staff.** This could be due to flaws in the system (v1), due to the lack of knowledge of users (v12) or to the complexity of medical data (v22). As a result, it is possible that the confidentiality, integrity and availability of the assets listed on the right could be breached.			A3. National Healthcare System 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 A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Health (I 02) = 4 - Legal (I 09) = 4	Very Low (10)

Reference	Risk			Affected Assets
R19	The system can be impacted on by several vulnerabilities that could cause a **risk of human error in cases of emergency**. These are flaws in the system (v1), lack of usability (v2), the important responsibility of the patient in the process (v3), the different level of treatments available depending on the country (v20) and the complexity of medical data (v22). In case this risk becomes a reality, the confidentiality, integrity and availability might be breached and the impact could be the following.			A1. Health / Life A3. National Healthcare System A5. Mobility of people 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 A14. Public health research data A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Health (I 08) = 4 - Legal (I 02) = 5	Very Low (10)

Reference	Risk			Affected Assets
R20	**A risk of non compliance with data protection legislation** could be generated by problems with the system (v1, v2, v4), by the lack of awareness of users (v12), by problems with consent forms and restrictions on the use of data (v16, v17, v18, v19, v21). It could impact on the confidentiality and on the list of impacts detailed below. It has a straight negative impact on patients / individuals (breach of their personal data) as well as healthcare companies (legal liability due to non-compliance with the legislation).			A3. National Healthcare System A4. Human rights and social values A6. Health card A7. Health monitoring devices 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
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	4	5	- Legal (I 02) = 5	Very Low (10)

Reference	Risk			Affected Assets
R21	**An inadequate provision or unavailability of medical services** could occur due to flaws in the system and its dependency on external infrastructures (v1, v4), the latter's lack of usability and convenience (v2, v6), non respect of legislation and regulation (v16) and differences between countries (v20). It could generate the following impacts and lead to a breach of confidentiality.			A1. Health / Life A3. National Healthcare System A5. Mobility of people A6. Health card A7. Health monitoring devices A8. Data collector / Home Hub A9. Personal IT equipment A10. Data centre and call centre A13. Electronic Prescription A15. Medical Procedures and Operational Standards A16. RPM Service / Disease Management Program A17. Hospital IT System
Risk Level	**Attack potential**	**Opportunity**	**Impact(s)**	**Risk Tolerance**
5	1	5	- Organisational (I13) = 5 - Health (I 09) = 4 - Financial (I 10) = 4	Very Low (10)

Prioritising the risks

The following table represents a classification of the risks by risk level. Given the numerous risk having the maximum risk level, the risks have also been classified by Impacts and then by probability.

Risk Number	Risk Title	Security criteria			Probability	Impact	Risk Level
		Confidentiality	Integrity	Availability			
R02	Having a system not compliant with informed consent legislation.	X			5	5	5
R03	Compromising the users' credentials.	X	X	X	5	5	5
R07	Damaging the equipment.			X	5	5	5
R09	Occurrence of a system malfunction and/or breakdown.			X	5	5	5
R11	Using the devices unprofessionally.	X	X	X	5	5	5
R14	Authorized individuals gaining access, modifying and/or deleting the patient's data.	X	X	X	5	5	5
R16	Using inappropriately the data for research or other purposes different than those they were initially intended for.	X	X	X	5	5	5
R19	Making error in cases of emergency.	X	X	X	5	5	5
R20	Not complying with data protection legislation.	X	X		5	5	5
R21	Providing inadequate medical services or medical services being unavailable.	X		X	5	5	5
R05	Compromising the availability of the service.	X		X	3	5	5
R08	Natural threats damaging systems.		X	X	3	5	5
R01	Not following the correct instructions for equipment use, treatment and medication.	X	X	X	5	4	5
R04	Breaching the confidentiality or the integrity of the data processed.	X	X		5	4	5
R06	Overloading the devices or the hubs.			X	5	4	5

Risk Number	Risk Title	Security criteria			Probability	Impact	Risk Level
		Confidentiality	Integrity	Availability			
R10	Stealing the patient's garment and/or IT equipment.	X		X	5	4	5
R13	Unauthorized individuals gaining access, modifying and/or deleting the patient's data.	X	X	X	5	4	5
R15	Data surveillance and profiling.	X	X	X	5	4	5
R17	Patient misinterpreting the data.	X	X	X	5	4	5
R18	Medical staff misinterpreting the data.	X	X	X	5	4	5
R12	Unauthorized people using the measurement devices.	X	X	X	3	4	4

Table 6 - Prioritised Risks

Glossary

Here are some definitions of the terms / concepts according to ISO/IEC 13335-1 (2004)[1] and the Glossary in ENISA Web-site[2] 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 organization (note: in our case not only the organization...). 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,
- 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.

---

[1] *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"*
[2] *http://www.enisa.europa.eu/rmra/glossary.html*

Availability – "The degree to which a system or equipment is operable and in a committable state"

Integrity – "ensuring data is whole or complete, data must be identically maintained during any operation (such as transfer, storage or retrieval)"

Confidentiality – "ensuring that information is accessible only to those authorized to have access"