‘Being diabetic in 2011’

Identifying emerging and future risks in remote health monitoring and treatment

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.

Contributors

This report presents the results of the risk assessment pilot performed in 2008 on a specific scenario regarding health remote monitoring and treatment. The report and the study was coordinated by the ENISA team, using input and comments from specific subject matter experts in the area, including industry, academic and government experts; notable some of these experts are already members of the ENISA Stakeholder Forum on Emerging and Future Risks. The content was collected via a mailing list, telephone conferences and face-to-face meetings.

This paper should not be taken as representing the views of any company or other organisation.

List of contributors (in alphabetical order)

Catherine Chronaki, Biomedical Informatics Laboratory at the Institute of Computer Science, Foundation of Research and Technology Hellas (FORTH), Greece

Claire Vishik, Intel Corporation, UK

David Wright, Trilateral Consulting, UK

Emilio Mordini, Centre for Science, Society and Citizenship, Italy

Evangelos Markatos, Foundation of Research and Technology Hellas (FORTH), Greece

Frederik Kortbaek, European Privacy Institute, Denmark

Guillaume Le Galiard, **Adèle Adam** and **Hervé Ysnel**, Logica, France

Hans Oude Alink, Ministry of Economic Affairs, The Netherlands

Julien Touzeau, Airbus, France

Milan Petkovic, Philips Research, The Netherlands

Mireille Hildebrandt, Vrije Universiteit Brussel, Belgium; Erasmus School of Law, Rotterdam, the Netherlands

Paul McCarthy, ESRC Centre for Economic and Social Aspects of Genomics (CESAGen), Lancaster University, UK

Contact details:

For more information on this report, you may contact:

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

Contents

Introduction

Since 2007, ENISA has been conducting a series of activities towards developing a comprehensive framework for identifying and assessing emerging and future risks (EFR). As a result of these activities, ENISA has constructed an EFR Framework. The EFR Framework is scenario-based and consists of certain phases for the formulation and analysis of scenarios, mobilisation of the necessary expertise (human resources) to assess and analyse the scenarios and leveraging of the management capabilities to collect and disseminate assessed information (e.g., scenario descriptions, threats, vulnerabilities, assets, impacts, risks, etc.).

The agency also sought to validate a European capacity for the evaluation of those risks to network and information security that may emerge in the near term, i.e. over the next three years. The work in this area is relatively new and, as such, calls for the interaction and co-operation of many leading experts from different disciplines, which is why ENISA established an EFR Stakeholder Forum and consulted with other subject matter experts. The EFR Stakeholder Forum, comprising partners and experts from industry, EU organisations and Member States, supports the agency in its deliberations on and assessment of EFRs and has contributed significantly to this pilot.

The pilot was undertaken in order to test and provide a "proof-of-concept" of the developed and proposed EFR Framework. It is based on a scenario in the area of remote health monitoring and treatment, an area which was selected after discussions with the EFR Stakeholder Forum. This report presents the results of the pilot exercise.

Why an e-health scenario?

The European Commission and some Member States have been actively promoting the merits of e-health in recent years. The Commission issued an e-health action plan in 2004[1] and, in July 2008, a Recommendation on cross-border interoperability of electronic health record (EHR) systems so that doctors can gain access to vital information on patients from other Member States whom they happen to be treating. It was also announced that it would co-fund a Smart Open Services (SOS) project (http://www.epsos.eu/) with 12

[1] *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. For more on the EC's e-health strategy, see 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. The ultimate goal is to enable access to the patient's electronic health record and emergency data from any place in Europe.*

Member States and their industry players, to demonstrate the benefits of such interoperability.[2]

The Commission has described e-health as the application of information and communications technologies across the whole range of functions that affect the health sector. E-health tools or solutions include products, systems and services that go beyond simply Internet-based applications. They include tools for health authorities and professionals as well as the delivery of personalised health systems for patients and citizens. Examples include health information networks, electronic health records, telemedicine services, personal wearable and portable communication and sensory systems, health portals and many other ICT-based tools assisting the prevention, diagnosis, and treatment of disease and illness, as well as health monitoring and lifestyle management to aid in the prevention of disease and illness.

Health care expenditure represents an increasingly large percentage of national budgets. Officials are interested in e-health in part because it can help to (1) limit costs and improve productivity in areas such as billing and record-keeping, (2) reduce medical error, (3) alleviate unnecessary care and (4) achieve savings in business-to-business e-commerce relevant to the health care sector.[3]

Nevertheless, e-health remains controversial and, some would say, risky. One of the biggest challenges in implementing e-health concepts is convincing the public that their electronic health records will be safe and secure. According to the Article 29 Working Party, electronic health records pose "significant challenges in ensuring that only appropriate health professionals gain access to information for legitimate purposes related to the care of the data subject".[4]

It was in this context that we considered a scenario on the issue of e-health and on remote health monitoring and treatment in particular would be an excellent subject of analysis, the results of which could also contribute to discussions at EU level and have direct policy relevance.

Moreover and based on all these considerations, Philips Research (Netherlands) produced a very interesting proposal for a scenario on remote health monitoring and treatment. The EFR Stakeholder Forum welcomed this proposal, which formed the basis for the scenario of the EFR pilot (for the complete text of the scenario, please refer to Annex I).

---

[2] *European Commission, "eHealth initiatives to support medical assistance while travelling and living abroad", Press release, IP/08/1075, Brussels, 2 July 2008.*

[3] *Cited in P.M. Danzon and M. Furukawa, "e-Health: Effects of the Internet on Competition and Productivity in Health Care", in The Economic Payoff from the Internet Revolution, the Brookings Task Force on the Internet, Brookings Institution Press, Washington, DC, 2001.*

[4] *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.*

The EFR pilot: objectives, scope and limitations

The pilot had two objectives:

- To identify major emerging and future risks of the particular area chosen (remote health monitoring)
- To obtain feedback on the EFR Framework, so that it could be updated and improved.

Once the topic of the scenario was identified, ENISA and Stakeholder Forum members discussed its scope and level of analysis. Eventually, it was agreed to have one scenario dealing with remote health monitoring and treatment. In addition, it was decided to identify all the major IT components at a somewhat high or strategic level and to group these into generic categories, as found in the "What are we trying to protect" section of this report and in the Asset fields of the EFR Application Scenario template (see Annex I).

A series of assumptions were made in the development and analysis of the scenario. They are explicitly detailed in the scenario template in Annex I. The assumptions were necessary in order to develop and analyse the scenario and then to identify the risks. The risks are factored into these assumptions, which means if the assumptions are changed, an identified risk may not be valid or an additional risk may emerge.

The scenario does not and cannot cover all possible aspects of this very wide area of applications and therefore the results produced are by no means exhaustive. It does, however, present some of the potential risks and challenges posed by emerging e-health applications. It is expected to contribute to the dialogue on e-health implementations and to fuel further study of these issues.

Objective and structure of this report

As mentioned above, this report presents the results of the EFR pilot conducted in 2008 and which deployed the ENISA EFR Framework in order to identify major risks associated with e-health generally and remote health monitoring and treatment specifically. Its major objective is thus to provide a high level overview of the results. Of the supporting documentation on which this report is based, the scenario template and the risk assessment report are annexed and the EFR Handbook can be found on the ENISA EFR website.

The report begins with a cautionary tale, which is based on the application scenario prepared by ENISA and its Stakeholder Forum. It provides a brief overview of the risks and challenges identified in the deployment of remote health monitoring and treatment programmes. The next two sections present the major risks identified in the course of the pilot and the assets, i.e., what we are trying to protect. Finally, the report concludes with a very brief overview of the methodology used, namely the ENISA EFR Framework, in order to identify and analyse the risks. The Annexes provide the detailed scenario template and the risk assessment report produced by Logica's EBIOS experts.

A cautionary tale[5]

Setting the scene – the actors – what's at stake – the drivers

Ralph knew it was going to be a tough three days. As expected, he was sparring with Fred, his tenacious, young opponent, an assistant deputy minister from the Finance Department, who was intent on derailing the health ministry's dream of an electronic health system for all citizens. Ralph's mission was to convince other conference delegates that the government should proceed with an operational system, while Fred was diametrically opposed.

There was a lot at stake – assumed improvements to the quality and availability of health care to the country's population versus the huge start-up costs and higher taxes at a time when economies had already been battered by the continuing effects of 2008's financial meltdown three years ago. Ralph and Fred seemed to take the debate to a personal level. In open discussions within the conference room, where the decisions were expected to be made this week, the animosity between the pair seemed palpable.

Ralph was in his late 50s, diabetic, mildly overweight, with thinning hair, frequently cleaning his spectacles with the end of his tie. His grey suit matched his somewhat sombre demeanour. He seemed to be the very embodiment of a bureaucrat. By contrast, Fred was young, fit and quick. Nevertheless, in the debate about whether an e-health system offered value for money, they seemed to be evenly matched. Participants from other government departments were struck by the apparent irony of the bureaucrat supporting deployment of innovative technologies while the ebullient Fred was doggedly resisting heavy new expenditures on anything. Sensing how undecided other participants were, Fred, seemingly as well briefed as his counterpart, was set on calling into question the integrity of the proposed e-health system.

Studies show advantages of e-health but…

"We are in favour of this e-health system. Several studies here and abroad have shown the advantages of e-health. We have consulted widely with the public over the past year and a majority are in favour of such a service…" said Ralph.

most people not aware of true costs and vulnerabilities

"Let me stop you there, Ralph," Fred interjected, shaking his

[5] *The scenario in this paper is based on the high-level scenario used in the assessment (please refer to Annex I).*

head. "I've seen surveys too and they show this majority to be very slender indeed. And, let's face it, most people are not aware of the true costs and vulnerabilities."

Pilot projects are useful

"We've had several pilot projects," Ralph protested, "and they show a very high level of user satisfaction."

"Yes, I've heard about those, and I've also read the experts' evaluation of them. In fact," said Fred, waving a copy of a report in the air above his head, "I have a copy here. And I'd like to highlight a few of the points the experts raised."

"Please do," said Ralph cautiously.

But there are still risks, e.g., data breaches and associated liabilities

"In the section on risks, the experts cite concerns about the security of the e-health system and the prospects for breaches in a system that would hold sensitive data on every person in the country. As an official of the finance ministry, I have grave reservations about the potential liabilities we could face if hackers were to penetrate a database with tens of millions of names. They could steal all those data or corrupt them or both. It's not just hackers that could test how alert your officials are, but suppose some of your staff get caught looking up the private medical records of their favourite politicians, sports heroes, rock groups and film stars. I can just see the headlines in the tabloids now." The loss of data on our citizens if such records were compromised would be disastrous, both for the lives of our citizens and their confidence and trust in our government.

Solutions, no matter how good, have not stopped determined hackers

As Fred spoke, Ralph thought about possible solutions -- access control procedures, a system that logs everyone who accesses every file, audit trails, experts to test vulnerabilities. Such safeguards sounded okay on paper, but no system is flawless or impregnable. No matter how good the security, it was just a matter of time before someone would figure out a way to break it.

Who should have access to electronic health records?

"Who is going to have the right to access all those electronic health records? Will it include insurance companies, employers, credit-checking companies? What about the Department of Motor Vehicles? Should they be allowed to know whether a prospective driver or some old fellow" Fred turned and smirked in Ralph's direction "who wanted to renew his licence was medically fit to have one?"

The risk of repurposing data (mission creep, function creep, secondary use)

"I also have concerns about how well officials in your department", here Fred pointed a long finger at Ralph, "could resist the temptation to reuse all those data for some other

purposes not explicitly stated when the data are collected from patients and doctors. For example, I can just imagine officials in your department dreaming up some new research schemes to tantalise their university friends. Or indeed some health-care company or department in the government may wish to collude with you, being unable to resist the lure of being able to research cure or deliver more efficient health care. This sort of mission creep always worries me, not just because of the liabilities we could face, but also because it is always, I mean always, incipient to growing bureaucracies."

Informed consent is a minefield of its own

"I agree," Ralph responded, "There's no doubt all those data will be a valuable resource, and that's why we have instituted strict informed consent requirements. If anyone has any bright ideas about reusing data, they must first get the data subject's informed consent." Even as he spoke, however, Ralph knew "informed" consent was a minefield. First, there was a definitional issue – what did "informed" really mean and how practical would it be to get when you had to "inform" thousands, perhaps millions of data subjects in order to get their consent. The UK government tried going down the route of "implied consent", but the Article 29 Working Party has said consent must be "freely given, specific and informed".[6] Ralph was also aware of the history of informed consent, and the failures and the ways in which it could be overridden for different purposes. Given the importance of trust in the system by citizens this could have disastrous implications for confidence in the entire project and the data being collected and stored.

Giving people the right to choose who could have access is riddled with problems.

"All good questions, Fred," replied Ralph, seemingly unperturbed. "Everyone will have the right to specify exactly who should be able to access their electronic health records. We will indicate options and rationales for those options in everyone's record, and everyone will be able to review and change their choices whenever they want." While this sounded good, Ralph knew there were problems, somewhat like the informed consent issue – some people would not take the time to understand the choices or their implications, some would be intellectually challenged and of doubtful competence to make such a determination, others would forget to check the validity of their choices in six months or a year.

[6] *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.*

The risk that the data will not be accurate

"Okay, fine, but here's another point. How can you ensure that the data in an e-health system will be correct? Lots of people travel abroad on business or holiday and receive medical attention while they are away from home. Isn't it possible that foreign doctors might misinterpret the data in patients' electronic health records or that our doctors misinterpret what those foreign doctors have done? Also there are already reports that our own health care professionals do not trust each other's own entries in existing medical records, with local doctors complaining about hospital staff and vice versa. How are we to ensure standards that everyone can agree on adhere to in recording patient information? Again, the ugly head of liability rears up."

Relying on individuals to ensure the accuracy of their data is an imperfect strategy at best. Developing an algorithm to check for accuracy is a good idea, of course, but as a bankable proposition, it is highly dubious.

"Of course, that's possible," Ralph admitted. "Anything is possible, but we will minimise those risks by encouraging every individual to review their electronic health records regularly and every medical practitioner to do the same. We are also trialling algorithms to automatically check for inconsistencies and anomalies in the EHRs." What Ralph did not say was how efficient and accurate the results were from the use of these algorithms. In practice, they were like facial recognition software – getting better, but achieving 100 per cent success ratios was an ever-receding mirage. Yet Ralph was convinced that while standardisation might be difficult it would be of benefit not only for this system but also across the health service in improving quality of care provided by health care staff and improving the experience of care on the part of patients.

While e-health schemes might make economic sense, it is important they enjoy public support. Otherwise, there is a political risk to policy-makers, an erosion in trust and confidence.

"Based on what some of your experts have written here," Fred poked the report for emphasis, "I wonder how much support this huge e-health scheme really enjoys among our fellow citizens – to whom we have fiduciary duty, I might add. While your report emphasises the economic benefits of this scheme, we have to wonder whether the concerns that groups have expressed about problems and risks with the system outweigh these supposed financial benefits.

Key stakeholders (doctors) are concerned about the informed consent issue as well as other issues. A balance must be struck between concerns.

Fred looked around the horseshoe-shaped conference table, nodding at each delegate as if to elicit a similar response from them. "Also, it seems a high percentage of physicians across the country are worried about getting informed consent from their patients before they enter any of their details into electronic health records for the delectation of your officials."[7] *Fred*

[7] *A survey by The Guardian found that 59 per cent of GPs were unwilling to upload any record without the patient's specific consent and were increasingly concerned about the government's plan to automatically upload the records of everyone who does not register an objection. According to The Guardian story, government ministers said unless someone objected, it would be assumed that they*

continued, "Indeed it is not just doctors that are concerned, patient groups are telling us they remain wary about shifting too much responsibility for care to individuals. Informed consent is key, yet even from your own report it remains difficult to see how you will balance these concerns in ensuring informed consent is given?"

Informed consent is not always possible. Fallback procedures are helpful, but require safeguards and oversight (how can we know that a guardian always acts in the interest of the patient?).

"Quite right too," said Ralph. "Informed consent is a prerequisite for initiating an EHR. Of course, informed consent is not possible in some cases, for example, children or those suffering dementia, so we have procedures for going to their guardians or legal representatives." Ralph does not volunteer information about those procedures, because some experts have questioned their adequacy and because he knows that the more stringent safeguards are, the more costly they are too.

Any system suffers the risk of externalities.

Fred wasn't to be slowed down. "Another point the experts raise is this. Let's suppose, against the odds and our better judgement that our political masters decide to go ahead with a full-blown e-health system. Paper records get chucked. Everything is digitised. Suppose then we had a true crisis, for example, that the avian flu mutates further so that it is easily transmitted from human to human. Then, let's suppose everyone is trying to get access to the e-health system at the same time, and what happens? It crashes. Then where are we. Also what happens if an individual's own device fails: from your report there are many risks where this may occur, such as an individual incorrectly operating this device, what then will be our liability, or even the public outcry if these technical failings lead to injury or fatality?"

Redundancy is no guarantee against systemic failure. Testing for worst-case scenarios is not the same as being able to cope with them. It is not possible to foresee all worst-case scenarios.

"Yes, that is a good point," Ralph seemed to agree, but added, "and that's why we are building in redundancy and testing for worst-case scenarios."

had given "implied consent". 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

The risk of a conflict of interest.

Fred smiled, lifted the report as if he were inspecting the fine print and then queried: "Finally, among the pilot projects mentioned here is one on remote health monitoring and treatment that involves employees in your department. Did you know that? How are we to trust the conclusions of this report then, is it not in the interest of your departmental officials to ensure the scheme is adopted?!"

Ralph makes a valid response, however, the exchange shows how easily information can be misinterpreted.

"On the contrary," said Ralph. "Our minister encouraged all employees to take part. He felt that if we were going to sponsor a national e-health system, then all of us should have first-hand experience with it. I agree and that's why I too volunteered to take part."

Remote health monitoring and treatment, using special technologies, such as a vest equipped with biosensors is theoretically a good idea, but costs to the individual must be taken into account. Ralph could afford such special items, but will everyone?

"In fact", Ralph chuckled, "I am wearing a special vest embedded with various biosensors." He ignored the scattered giggles from the other delegates and carried on with his explanation. "The sensors are part of what's called a body area network. They monitor my vital signs and my watch collects the data and then transmits it to a data collector hub which encrypts this information and then transmits it over the Internet to my physician. In fact, she's quite pleased that I'm taking part in the trial, because I have type II diabetes and, as you can see, I'm overweight, this system helps with my condition and the regular monitoring has helped me keep to an exercise and proper diet, for which my family is quite thankful" Ralph patted his tummy, and his fellow delegates, most of whom were also overweight, laughed appreciatively.

Is there a risk that the costs of monitoring and treatment will short-change prevention?

If there are delays in implementation of the system, there is a risk that "payback" may be much longer.[8]

"Like many of my generation," he added, "I suffer from high blood pressure and diabetes. I regret to say that monitoring and treating me and others of my cohort account for quite a high percentage of the national health budget. In fact, it's one of the reasons why I'm personally keen on the new e-health scheme. You might not believe this, but I'm convinced that in spite of the high start-up costs, the system will pay for itself within five years maximum." Ralph thought back to predictions of this made in 2009 when a colleague of his from the UK spoke of his national

[8] *In late January 2009, the UK House of Commons public accounts committee (PAC) warned that key parts of a £12.7 billion programme to upgrade the NHS's information technology are on the brink of failure. The NHS is currently forecasting a completion date of 2014-15, four years later than originally planned. MPs said even this revised schedule looks over-optimistic. See Carvel, John, "New NHS computer system on brink of failure, warn MPs", The Guardian, 27 Jan 2009. http://www.guardian.co.uk/society/2009/jan/27/nhs-it-computer-programme-health-public-accounts-committee*

health service spending over one million Euros a day on care and treatment of Type 2 Diabetes with 4% of the population affected. Things had not improved since then[9]*.*

Like most technologies today, there is a risk of loss, theft and accidental damage. Ralph says nothing untoward has happened to him – yet – but the past is an unreliable guarantee to the future.

Fred was curious. "What happens if you send your vest to the dry-cleaners and they damage the sensors or they lose it altogether or give it to another customer by mistake?"

Ralph chuckled. "No, the sensors are quite impervious to the laundry, and I've never lost it. But even if I did, the manufacturer has told me that the costs of these garments will be only slightly more in comparison to vests without the sensors."

"Is there anything else you have to do in this project besides wear a special vest?" Fred appeared genuinely interested. His normal sarcasm seemed to have evaporated.

Health monitoring and treatment cannot eliminate all risks. The individual must do his bit too.

"A few things. I have to follow the treatment regime prescribed by my doctor – which means doing some exercise every day. I go for a brisk walk, and I come to the gym to work out on the exercise bikes. I follow a strict diet. Oh, yes, and I have to maintain an online health journal."

"Oh, yeah? What's that? That sounds a bit of bore."

"No, it's not actually. It's like keeping a journal as well as recording measurements. But I like to be able to read and have a sense of control over my own medical information. I also make sure the data collection hubs in my home and office are functioning. My care centre also sends daily reminders to my mobile to make sure I take my medication. I have to respond to those. That's more or less all I have to do."

[9] *http://news.bbc.co.uk/1/hi/health/7905734.stm*

E-prescribing is a good idea but only a tiny percentage of doctors actually use such systems.[10] There are also risks, e.g., if a doctor delegates the e-prescribing to a nurse or assistant who abuses it.

"My physician was willing to participate in the pilot project, to see how it might make her own practice more efficient and less error-prone."[11]

"Less error-prone? How do you mean?"

"Well, for example, all her prescriptions now are made electronically. It does away with her scrawl. She decides what I need and then sends the prescription electronically to my local pharmacy and sends me a copy. I don't have to hang about at the pharmacy either. The prescription is there, ready for me to pick up. Also because my health record is viewable by me at any time I can also review my doctor's comments. Also because they are standardised should I be treated by any other doctors I can review and understand their comments much easier as well. I feel much more in control and involved in being responsible for my health and well-being"

If a paramedic could get a reading off Ralph's health card, then an unauthorised person, e.g., a hacker, could too.

Ralph carried on: "I have an updateable health card, which has my personal data and latest health emergency data. So if I travel somewhere and fall ill, I could just present my health card or, heaven forbid, if I was in accident and fell unconscious, then the paramedics could just dig out my card and get a reading off it to know whether I am allergic to anything, penicillin, for example." Ralph stopped and looked at the delegates one by one, as if to make sure they understood what he was saying. Fred interjected however, "Doesn't this mean however that you depend on these places to also be digital? What happens if no electronic record is kept of this treatment?". "This is a concern of course, but it is also a question for our partner countries as our frameworks must be interoperable at some level" replied Ralph.

A history of failures and delays undermine the benefits advocated by enthusiasts

Some delegates nodded, others began talking to each other. Ralph and Fred could see that everyone was tired; it had been a long day of duelling, of thrusting and parrying, but neither opponent had made a decisive cut. It was time to call it a day. Ralph glanced towards Fred, who was just answering a clearly unsettling call, judging by his heavy frown and his loosening the knot of his tie. Fred's face turned ashen. "I'm on my way," he said to the phone. He turned to Ralph and then to the delegates and explained tersely. "It's my father. He is a diabetic and just

---

[10] Only two per cent in the US. See Connolly, Ceci, "Few Doctors Sign Off on Online Prescribing", Washington Post, 25 Nov 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/11/21/AR2008112102939.html

[11] Most doctors are already using information technologies. See, for example, the report prepared for the European Commission (DG Information Society and Media), entitled 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

had a stroke and is in a critical condition at the hospital". It seems he was walking outside his village and he collapsed. There was some delay before anyone found him. He had no way of communicating his condition…." Fred's voice trailed off,. "I've got to go," he said, "I'm sorry." As he opened the door to leave, he turned and said, "If my father had been wearing a vest like yours, Ralph, perhaps he would have had the warning he needed before falling ill."

A sad event triggering some thoughts…

The next day, the last of the conference, Fred did not show up, but he had left a message for the participants, which the chairman read out: "The problem that confronts my family prevents me from joining you today. It has become apparent to me that if my family had been using some of the technologies we have been discussing the last two days," – a murmur went though the conference room as the chairman read these words – "this incident may have been avoided and I could have been with you today. I wish you well in achieving a consensus."

Caution seems to be the prudent answer at this point: the benefits are clear, but also the risks entailed cannot be ignored

The chairman having read the message, eyed Ralph and raised his eyebrows. Ralph cleared his throat and stood up. "Dear all, I will be brief. First, though, I move that we send a unanimous message of support for the difficult family situation faced now by Fred." Everybody nodded. Ralph went on: "We have had two days of animated discussion, but we seem not to have reached a consensus. You have heard many pros and cons, benefits and risks arising from e-health and remote health monitoring and treatment. While the benefits seem laudable, as Fred has now acknowledged under unfortunate circumstances, I find that I cannot just brush aside Fred's concerns: the costs, risks and history of delays and failures of other similar systems cannot be overlooked." He paused as if reflecting upon the irony of the situation: he had convinced Fred, but Fred had convinced him. He then said, "Perhaps caution is *the best approach just now. Maybe we need to assess whether, in addressing some problems, we are creating others of a different nature, whether cost over-runs and delays would fatally undermine the credibility of the system." Ralph sat down and slowly began cleaning his glasses with the end of his tie.*

The chairman assented with a slight smile as delegates decided against immediate implementation, but in favour of more detailed studies of the risks.

The risks

This section lists major risks, also mentioned in the preceding cautionary tale that were identified based on the scenario of the EFR pilot and which Ralph and other stakeholders might encounter in relation to remote health monitoring and treatment services. Some of these risks affect only the individual (e.g., Ralph), while others could affect *all* users. The risks mentioned in this section are listed according to their risk level (high), impacts and probability. The risks were identified in a collaborative effort by ENISA, representatives from its EFR Stakeholder Forum and external subject matter experts.

1. Failure to comply with informed consent legislation

An e-health system will collect lots of data about citizens and it may be difficult to know precisely who should have access to those data, for what purposes and when the citizen's informed consent should be obtained. Even the notion of what constitutes informed consent could vary according to the circumstances of specific contexts. In some cases, informed consent could be intrusive or difficult to obtain. This also in turn poses challenges for data protection, the secondary uses of data and how to comply. There is the perception as such that medical data is different from other personal data, often in the eyes of both governments in member states and citizens of member states.

2. Failure to comply with data protection legislation

A failure to comply with data protection legislation, such as the European Data Protection Directive (95/46/EC) and the e-Privacy Directive (2002/58/EC), may happen because someone is not aware of what their obligations are. Furthermore, while Member States have transposed the Directives, there are variations in the way they have done so.

3. Data breaches

There is always a risk that the confidentiality or integrity of the patient's data could be breached. Evil-doers could eavesdrop on communication between the patient and a doctor or steal or otherwise appropriate personal data. Evil-doers could, of course, be "insiders". In addition, officials and patients may be negligent or careless or insufficiently careful in handling personal data and may lose such data.

Someone without authorisation, who could be an insider, could gain access to Ralph's personal medical data, modify or delete the data because the access control measures are inadequate, because the data have not been encrypted or otherwise secured. Likewise with such an amount of data being collected and stored, and the different levels of access as well as the number and variety in actors who have access to all or parts of the data, then the risks of accidental loss increase exponentially. Loss of data through accidental or mere incompetence in respecting data protection regulations are well documented across the EU.

4. Repurposing or secondary use of data (mission creep)

An e-health system or some component thereof, such as a remote health monitoring and treatment system, will collect and store an enormous amount of data. Because those data exist, there will always be a strong temptation to use them for a purpose different from that for which the data were originally collected – which would be a contravention of the European Data Protection Directive (95/46/EC). Such repurposing of data need not always be for nefarious reasons. Sometimes, it could be as "innocent" as researchers' wanting access to the data for purely scientific reasons which could result in successful treatment of a heretofore intractable disease, for example.

5. The user could be compromised

Ralph might use his equipment in an unprotected environment or over an unsecured communication channel. The e-health system might not be able to authenticate him and, consequently, would deny him service.

6. Equipment is damaged

Ralph's equipment could be damaged in a multitude of ways, through negligence or carelessness or accidentally or because he might use it in an inappropriate way because he is not aware of certain system requirements. It is unlikely that Ralph would use his equipment in an unprofessional way, but some users might.

7. Disruption of the service

Some flaws in the system design and/or infrastructure could lead to a malfunction or breakdown in the system, thereby disrupting service to users. Adding new functionalities to system design can also lead to delays in implementing new systems.[12]

A natural event, such as a hurricane or earthquake or forest fire, could damage the infrastructure on which the remote health monitoring and treatment system depends.

Ralph might find that his device or the system itself fails when it becomes overloaded, because the device is of low quality or the system infrastructure is not robust enough to cope with periods of heavy demand.

8. Theft

There is always a risk that someone might steal Ralph's sensor-embedded garment, health card or other information technology which he uses to take advantage of the remote monitoring and treatment service. The cost of the garment and/or user device might be relatively low, but the theft might happen at a critical time when he is very dependent on the devices, so that a loss of even a day or less could put his health at risk.

---

[12] *This seems to be happening in the case of the UK's e-health system. Carvel, John, "New NHS computer system on brink of failure, warn MPs", The Guardian, 27 Jan 2009. http://www.guardian.co.uk/society/2009/jan/27/nhs-it-computer-programme-health-public-accounts-committee*

9. Inadequate provision or availability of medical services

The remote patient monitoring and treatment service may not be available everywhere, at least, not at the same level of service. This could conceivably occur and be problematic at a number of different geographical levels, for example within the member state, between different member states and between the EU and other regions and external countries.

10. Human error in emergencies

Human error can occur anywhere at any time, but the ramifications are greatest in emergencies, exactly the time you don't want them to happen. Human error in times of crisis is problematic but given that adoption of the system may be widespread the risks of 'routine' errors precipitating crises must also be considered.

11. The patient might misinterpret the data

Ralph might misinterpret the data generated from his device or from the e-health system or his physician. Not everyone is as computer literate, intelligent or endowed with common sense as Ralph, thus, the risk of their misinterpreting data is that much greater. The data may be too complex or incomplete for Ralph or other patients to understand properly. This risk will be greater if more responsibility is shifted to the patient for maintaining his or her own electronic health record and, more generally, their health.

12. Medical staff might misinterpret, modify or delete patient data

Given the inevitability of human error, there is always a possibility that someone with authorised access to Ralph's data might misinterpret, modify or delete them, either intentionally or accidentally. This could be due to flaws in the system or a user's lack of knowledge or the complexity of the data or a mistake in the data.

13. Users may not follow instructions

Users may not follow instructions because their equipment is not user friendly or their treatment may depend too much on other components of the e-health system or they may simply forget to take their medication (or may not want to).

An evil-doer or even someone who isn't aware of the implications of what they are doing might use Ralph's monitoring device without his or anyone else's authorisation which, in turn, could result in the device performing badly.

14. Data surveillance and profiling

Insurance companies, employers, credit-checking companies, researchers and/or others may successfully engage in data surveillance (aka dataveillance) and profiling because Ralph's data have not been secured well enough or because access control measures are weak or are too "porous" (i.e., they do not do a good enough job in filtering out those who shouldn't have access to the data from those access is legitimate). A part of the problem here is the incidental data that might be gathered from the sensors. The most obvious of

these would be location, knowing the location of the patient in times of emergency is a critical element of the system yet knowing the location of the person at any given time could be of interest to example law enforcement actors investigating crimes. As with any form of data collection, and given the amount of data such systems will collect, it is also difficult to predict what uses or value data might have after it has been collected. Future scenarios might occur where data was then re-used for a purpose the system was not designed for.

What are we trying to protect?

This section identifies the assets that we are trying to protect against the risks mentioned above. Those "assets" may be tangible or intangible, owned by Ralph or his doctor, hospital, health care call centre, the National Health Service or others. Assets include any devices, technologies, applications, processes, data or anything of value to the individual, organisation or, indeed, society. Some assets are more valuable than others, of course, and those values may vary over time and/or according to the context. A glass of water may not have much value for most of us, but for the straggler crawling across the desert; it might be of enormous value. Similarly, aspirin is as cheap a medicine as exists, yet for the person suffering from an incipient heart attack, 300 mg of aspirin can make the difference between life and death. Assets have vulnerabilities which can be threatened or attacked[13]. Risks may have impacts on business operations resulting from unauthorised disclosure, modification or repudiation of information, or unavailability or destruction of information or service.

Identification of assets may seem straightforward at first, but in practice and as is detailed in the scenario analysis is more complicated after a sustained examination is made. After discussions within our working group, we agreed that in the context of our scenario, we are aiming at protecting the following:

- *Health and life* – refers to the physical and psychological condition or well-being of an individual and the absence of disease. Inadequate protection will result in deterioration of an individual's health and may even lead to loss of life.

- *Human rights and social values* – includes privacy, non-discrimination, dignity, social inclusion and e-inclusion, trusted human relationships, etc. They are important to us all as patients, individuals, family members, friends and to society. Persistent violation leads to a dysfunctional society, crisis and a breakdown in social order which in turn can lead to health problems which are psychological as well as physical.

- *Autonomy* – A person, like Ralph, who is afflicted with a disease or disability (in his case, diabetes and high blood pressure, which greatly increases his risk of a heart

[13] The International Organization for Standardization (ISO) defines **vulnerability** as a weakness of an asset or group of assets that can be exploited by one or more threats. It 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. **Threat** is defined as 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 unauthorised 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. Threat characteristics include motivation, e.g., financial gain, competitive advantage, frequency of occurrence, likelihood, and impact. See 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".

attack or stroke), can regain a measure of autonomy through the use of technologies as mentioned in the scenario. On the other hand, becoming dependent on monitoring technologies can be seen as a threat to autonomy.

- *National healthcare system* – provides healthcare and medical services to people at a reasonable cost. Poor or improper provision of services could lead to a deterioration of citizens' health and/or to loss of life.

- *Mobility* – refers to the ability and potential of people (individuals, patients, doctors, health professionals) to move across countries and be provided with comparable quality of healthcare and information society services wherever they are.

- *Personal data* – has at least two values, one that Ralph (or we) ascribe to his (our) own data and second, the value that someone else ascribes to it. That "someone else" can be a friend or a foe, a bureaucrat routinely gathering tax or health or demographic data as part of his job or an enterprise fuelled by personal data, needing to "personalise" the products or services they market to us or an evil-doer who wants our data to exploit them, to siphon off the savings from our bank accounts or to make large purchases in our name or to spam us about stuff we neither need or want. Ralph's personal data, like ours, can be found in a number of places – in his electronic health record, health journal, health card, his own laptop, in hospital databases, in his local pharmacy, in his doctor's files as well as in hundreds of other places (banks, insurance agent, tax department, local Council, etc.) The more places in which our data can be found, the greater is the number of people we can assume have access and the greater the risk is that someone will misuse or abuse our data.

- *Health cards* – contain encrypted data used for authentication, possibly also for digital signatures. Each individual has his own health card. While the identity information on the card cannot be altered, the medical information can be and is expected to be read by doctors or paramedics (especially in an emergency) who, if necessary, can verify the medical data stored on the card by means of a medical examination.

- *Health monitoring devices* – include items such as Ralph's vest embedded with biosensors. They measure blood pressure, weight, blood glucose levels and other parameters and send data to a home hub which in turn relays the data to a patient monitoring call centre. The integrity and quality of the supplied measurements must be reliable, otherwise faulty measurements have the potential to seriously affect the health or even life of the patient.

- *Personal information technology equipment* – includes items such as laptops or workstations, digital cameras, telephones and videophones. Patients, doctors and health practitioners use these as access points to the monitoring and treatment service and to enable tele-consultations. They may contain personal and sensitive data.[14]

[14] For Information about device interconnections, see
Bluetooth Medical Device Profile Specification
http://www.musenka.com/info/doc/MDP(MedicalDevicesProfile).pdf
USB Personal Healthcare Device Class Specification
http://www.usb.org/developers/devclass_docs/Personal_Healthcare_1.zip

- *Data centres and call centres* – are the nerve centre of the monitoring and treatment service. Data centres are independent organisations which manage medical data on behalf of a hospital or health plan and are tasked with ensuring security, privacy and resilience as a trusted third party. Call centres are typically staffed by nurses and other health care practitioners, who create patient monitoring reports for Ralph, his physician and others like them with similar needs and who are authorised to access the data or reports derived from it. The call centres respond to alarms triggered by Ralph's biosensors' detecting any abnormalities in his health signs. They would notify Ralph, his physician, emergency services and possibly next of kin. The call centres operate a Remote Patient Monitoring (RPM) Service and Disease Management Program, which may be regarded as the core service described in the scenario, i.e., monitoring and treating patients remotely. If this asset (a viable service) were compromised or disrupted, it could mean no care for Ralph and others like him, which in turn would undoubtedly lead to serious health problems for many and significantly damage trust and confidence in the system.

- *Electronic health records (EHR)* – contain health information including prescriptions and personal data inputted and confirmed by health professionals.[15] EHRs may also contain personal data automatically gathered by sensors (including patient location). In theory, EHRs are confidential, but sometimes law enforcement authorities (for example) will seek access to such data to help in solving crimes. In Sweden for example, the national biobank was supposed to be off-limits and its informed consent procedures were based on this premise, yet police gained access and were able to retrieve the data needed to locate and identify the killer of Foreign Minister Anna Lindh who was fatally stabbed in a Stockholm department store in 2003. Some experts have estimated that today's health records are seen not only by the patient and his or her physician, but also by hundreds if not thousands of call centre, hospital, medical and administrative staff as well as others such as those in pharmacies, insurance companies, our employers, etc. Electronic health records will increase the ease with which such data can be accessed and probably the numbers of people who can access them as well as increase the number of places where data can be accessed.[16]

- *Health journal* – used to record health measurements and personal data, analyse trends and provide feedback. Data entered by the patient and health monitoring call centre are reviewed by doctors. Some of the data can be consolidated and accepted into the EHR.

- *Electronic prescriptions* – will do away with doctors' notoriously difficult-to-decipher hand-writing. Doctors will send prescriptions directly and electronically to pharmacies,

[15] The Standing Committee of European Doctors (CPME) defines electronic health record as "a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual and the medical procedures done in electronic form and providing for ready availability of these data for medical purposes". http://www.cpme.eu. The Art 29 Data Protection Working Party adopted the same definition in its Working Document referenced above (see footnote 5).

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

insurance agents for reimbursement and, if necessary (for example, if the patient was hospitalised or fell ill in another country) to the patient's own physician. The e-prescriptions could include some personal data and a summary of the diagnosis to justify the prescription.

- *Public health research data* – preferably easily available and in abundant quantity, are needed for epidemiological research. An e-health system would greatly facilitate the research efforts of public health research institutions and governments. Consent procedures would have to be clear on this, and sufficient data protections would need to be in place and respected in order to remove all identifiable data from the records to be used in such research.

- *Hospital information technology systems* – store electronic health records and exchange data with the call centre, physicians and emergency services.

- *Networks* – are the backbone of any service provided to or on behalf of people. The basic (fixed) communications network enables telephony and data exchanges and so do the mobile phone neworks. New wireless networks have been emerging in recent years, e.g., WiFi and WiMAX. Networks employ a range of technologies including the venerable twiseted copper pairs, coaxial cable, fibre optic cable, radio waves, satellite and so on. Networks can be disrupted easily and too frequently[17], but *usually* (but not always) there is adequate redundancy or alternative routings to solve most such disruptions.

[17] For a recent example, see Ahmed, Murad, "India suffers massive internet disruption after undersea cables break", The Times, 19 Dec 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5372294.ece

Methodology

As mentioned in the introductory section above, during 2008, ENISA worked on building a framework to identify emerging and future risks ("EFR Framework").

The framework follows a scenario-based approach, where scenarios are used to present a particular case of the chosen technology and/or application and/or topic in order to identify the emerging and future risks. Once identified, the scenario data are subsequently analysed by using existing risk assessment methods. The following diagram presents a high level overview of this approach:

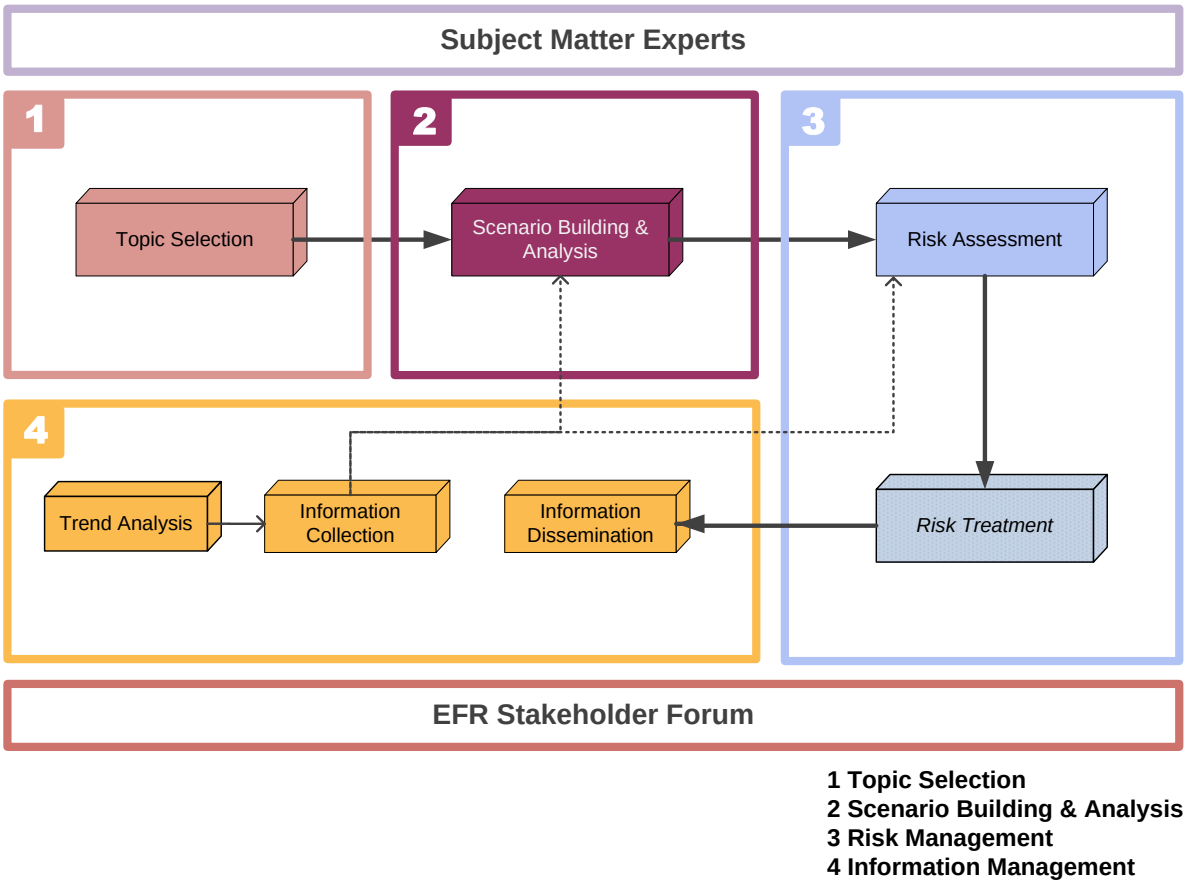

Figure 1: High level overview of the EFR Framework

In the beginning, the topic, namely the particular technology and / or application to be assessed is selected, based on proposals we receive from our stakeholders (industry, academia, Member States, EU Institutions). After the initial identification of the topic, the scope will need to be defined, as well as which areas to target in the possible scenario

(especially if the topic, technology selected is too broad)[18]. In the building of the scenario, the following items need to be considered and specified (please refer to Annex I):

- ***An introduction*** – provides an overview and background for the scenario.
- ***The scenario*** – includes the scenario "script" or story or the imagined future as well as a set of assumptions underpinning the scenario.
- ***Framing the scenario*** – is a way of deconstructing the scenario into its component elements on the basis of which an analysis can be made of the issues raised by or implicit in the scenario. The key elements are[19]:
  - *Timeframe* – How far into the future is the scenario situated?
  - *Location* – Where does the scenario take place, not only in geographic terms but also in its social context, e.g., in the home, at work in the community, etc.?
  - *Actors* – Who are the principal actors in the scenario? Whom do they represent?
  - *Technologies and/or devices* – What technologies or devices are used in the scenario?
  - *Applications* – What applications are referenced?
  - *Data* – What data are collected, for what purpose and who has access to them? Are the data repurposed or shared or passed on to third parties?
  - *Drivers* – What impels the actors? What are their motivations? What social, political, economic or other forces create or drive the situation described in the scenario?

- ***Analysing the scenario*** – The scenario is at this stage further analysed in order to identify, "extract" all the elements needed in order to proceed with the risk assessment and management. The elements to be identified in this phase are:
  - *Assets (tangible and intangible)* – What assets are mentioned or implicit in the scenario?
  - *Vulnerabilities* – What vulnerabilities are apparent or can be perceived in those assets?
  - *Existing controls* – What controls appear to be in place or could or should be put in place to safeguard the assets, especially in terms of their vulnerabilities?
  - *Threats* – What threats are referenced in the scenario or are implicit or can be imagined?
  - *Impact* – If the assets are attacked or compromised in some way, what would be the impacts?
  - *Acceptable risk level* – Given the probability of a risk and its potential consequences, what is regarded as an acceptable level of risk?
  - *Assumptions* – What assumptions have been made or seem apparent in the scenario analysis, e.g., in terms of the vulnerabilities, threats, impacts and risk acceptability?

The report at Annex I show how this structured analysis works in practice.

---

[18] *Please note that for a more detailed description of the EFR Framework you may refer to the ENISA EFR Handbook, soon to be published and will be available for download from our website.*

[19] The structure for framing the scenario is based on that developed for the "dark scenarios" in the SWAMI project. See Wright, David, Serge Gutwirth, Michael Friedewald et al., *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.

After an initial identification of the elements described above, we proceeded further with a more in-depth risk assessment. Any risk assessment methodology can be used at this stage, since the elements identified above are generic and may be used with the majority of the risk assessment methodologies. For the purposes of our study, we used the EBIOS Risk Assessment methodology, appropriately assisted by EBIOS experts from Logica, France.[20] The result of these activities was basically a list of possible risks posed by the technology and/or applications under study; furthermore, controls may be identified and recommended in order to address those risks.

The principal steps taken by the EBIOS experts to identify and assess the risks were the following:

- *Formulating the risks* – For each threat, a risk has been produced. In this study, each risk has its own box, which lists the vulnerabilities that can be exploited and security criteria concerned by the risk, and the affected assets. The following steps complete the details for each risk box.
- *Valuating assets and setting of tolerance levels* - Assets are assigned a value and the risk tolerance levels are set, which corresponds to the risk levels we are willing to accept, without implementing any measure or control to address the risk
- *Calculating the probability*, t*he attack potential*, t*he opportunity* and t*he probability* according to EBIOS methodology in order to evaluate the vulnerability and threats.
- *Identifying and valuating the impacts*
- *Determining the risk level*

For the full risk assessment report produced by the EBIOS experts of Logica (please refer to Annex II).

[20] EBIOS is the acronym for Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Objectives).

Annex I: EFR Pilot – Scenario Building and Analysis Template

Please refer to accompanying document.

Annex II: EFR Pilot – Risk Analysis Report

Please refer to accompanying document.