

Privacy Risk and Harms Assessment with the PRIAM Methodology



UiO :

Group Assignment 4B UiO - Department of Informatics

Andreas Nygård Ljøterud, Hemel Howlander, Malte Hansen

October 31th, 2022

Contents

1	Introduction	1
2	The PRIAM methodology	2
2.1	Information Gathering Phase	2
2.2	Risk Assessment Phase	3
3	Privacy Harms in an Example of a Medical Breach	6
3.1	Scenario	6
3.2	Privacy Harms	6
3.3	Discussion	7
4	Conclusion	8

List of Figures

1	The PRIAM methodology process.	2
2	Categories with their associated attributes.	3
3	Harm tree example.	3
4	Exploitability and risk source favoring.	4
5	Likelihood measurement scale.	4
6	Harm tree with computed likelihood.	5

List of Tables

1	Examples of harms of the UCLA Health breach and their attributes .	7
2	Relative impact of categories of privacy harms in the UCLA Health breach	7

1 Introduction

Since the introduction of the General Data Protection Regulation (GDPR) [4] in 2018, privacy impact assessments (PIA) have become a mandatory part of development cycles for products including collection or processing of personal data.

As the conduction of PIAs has not been the focus of most organizations before the GDPR, not a lot of solutions are public today. However, some approaches for specific applications exist (e.g. [3][2]). To provide a more general, systematic solution to PIAs the PRIAM methodology [1] was developed. To get a better understanding about privacy risks, their evaluation, and consequences we want to take a deeper look into the PRIAM framework and its applications.

In this report we will briefly present the PRIAM methodology, followed by a use case based on an example of a medical breach. In this example we will focus on the *privacy harms* resulting from the breach and discuss the information PRIAM provides us about the harms and their consequences.

2 The PRIAM methodology

In this section we aim to introduce how the PRIAM methodology works on a high level. In order to achieve this we will first provide a bird’s-eye view of the steps involved and then briefly explain what each step entails.

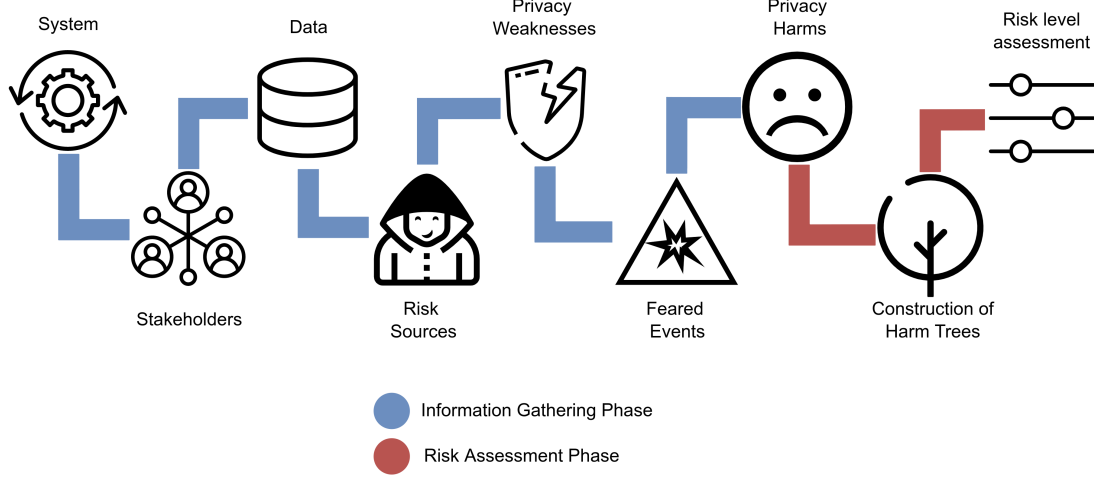


Figure 1: The PRIAM methodology process.
The PRIAM methodology process¹.

The PRIAM methodology process (see Figure 1) is split into two phases, the first of which being the *Information Gathering Phase*. The main objective in this phase is to gather the relevant information needed in order to accurately carry out the risk assessment activities in the *Risk Assessment Phase*.

2.1 Information Gathering Phase

As the foundation for the upcoming risk assessment, it is essential that the information collected in this phase is complete. To reduce the likelihood of an analyst missing aspects that may have an impact on privacy risks, the framework defines seven *components*. These components, namely the *system*, *stakeholders*, *data*, *risk sources*, *privacy weaknesses*, *feared events* and *privacy harms* are each associated with a set of *categories* and *attributes*. A category is essentially a list of elements relevant to a specific component, while attributes describes the characteristics of a component that may affect privacy risks[1].

In Figure 2 an example is given to illustrate this concept further. The potential or capability of the risk source, in this case the *Hacker* (which is the category), would be determined by the assigned values of its attributes. Similarly for *Health data*, which is a category of the *data* component, the attributes could indicate a potential privacy weakness. The categories and their corresponding attributes are however not only used for indicative purposes, but for constructing harm trees and calculating risk levels in the next phase.

¹All icons used are from <https://thenounproject.com>

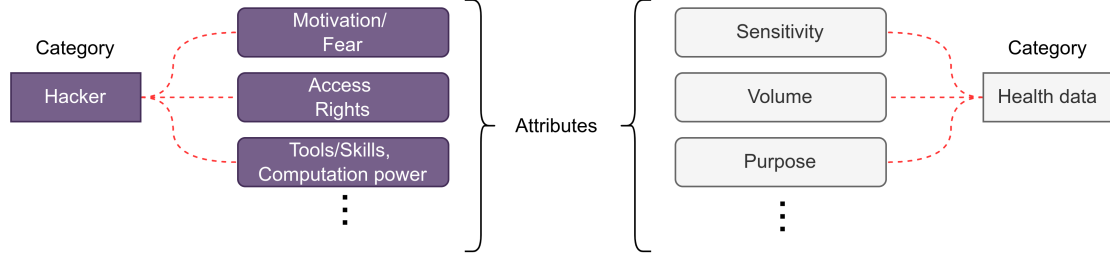


Figure 2: Categories with their associated attributes.

2.2 Risk Assessment Phase

With basis in the information collected in the *Information Gathering Phase*, we are set to perform the risk assessment. In order to calculate the risk levels associated with a given scenario, so-called *harm trees* are constructed.

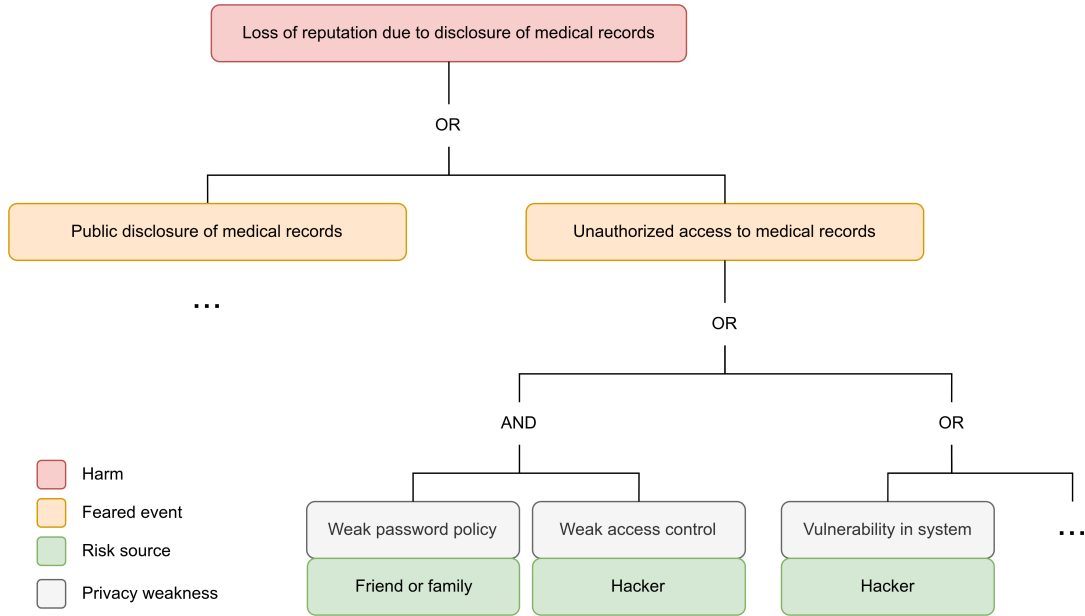


Figure 3: Harm tree example.

Harm trees (see Figure 3), similarly to attack trees commonly used in computer security[1], are used to describe the relationship between a privacy weakness, a feared event and a harm. The root node of such a tree will denote a harm, with branches leading to feared events that may lead to the harm in question. The leaf nodes denote privacy weaknesses and are represented by a pair consisting of the most relevant risk source coupled with a privacy weakness. In order to specify whether multiple events are required for an event to take place, the keywords **AND** and **OR** are used as decorators on the connecting paths between the nodes.

The risk levels for a given scenario, in this case the scenario previously given, is then calculated in the following way[1]:

1. Find the value of *exploitability* for each leaf node in the harm tree.

The *exploitability* value is defined in the previous phase, and denotes how easy it would be to exploit a particular privacy weakness based on relevant system attributes. For simplicity and illustrative purposes, we have assigned the value medium to all three in this case.

2. **For each exploitation, choose the values of the relevant attributes of the risk source most likely to exploit the privacy weakness leading to the harm.**

In order to calculate the likelihood of an exploit occurring, the characteristics of the risk source should be accounted for. In other words, does the profile² of the risk source favor an exploitation or not. In the case of *Friend or family* the majority of attributes does not favor an exploitation, while we consider the opposite to be true for both cases involving the *Hacker*.

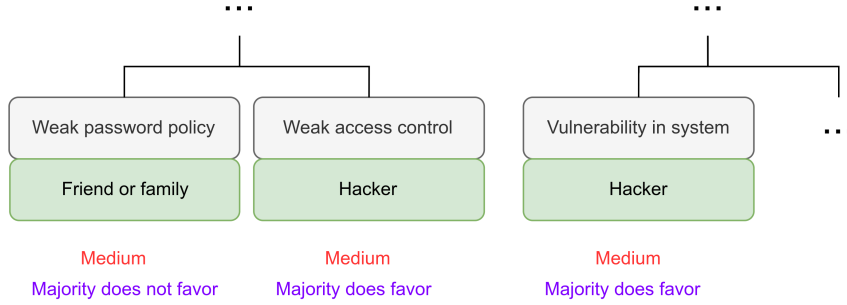


Figure 4: Exploitability and risk source favoring.

3. **Find out the likelihood of each of these exploitations from the above exploitability value and values of the relevant risk source attributes**

Likelihood of exploitation	Exploitability of privacy weaknesses	Relevant risk source attributes
Negligible	Low	Majority do not favour
Limited		Majority favour
Intermediate		All Favour
Limited	Medium	Majority do not favour
Significant		Majority favour
Maximum		All favour
Intermediate	High	Majority do not favour
Maximum		Majority favour
Maximum		All favour

Figure 5: Likelihood measurement scale.

The measurement rule used in PRIAM to determine the likelihood of exploitation can be seen in Figure 6 above, which means that the likelihood of our chosen exploitations are *Limited*, *Significant* and *Significant* respectively.

4. **Compute the likelihood of each feared event and harm according to the following rules, where P_i is the likelihood of i th child node:**

²Value of exploitation, motivation/fear etc.

- AND node with independent child nodes: $\prod_i P_i$.
- AND node with dependent child nodes: $\text{Min}_i(P_i)$.
- OR node with independent child nodes: $1 - \prod_i (1 - P_i)$.
- OR node with dependent child nodes: $\sigma_i P_i$.

In order to compute the likelihood of the feared event and ultimately the harm, we simply apply the rules above to each level of the tree.

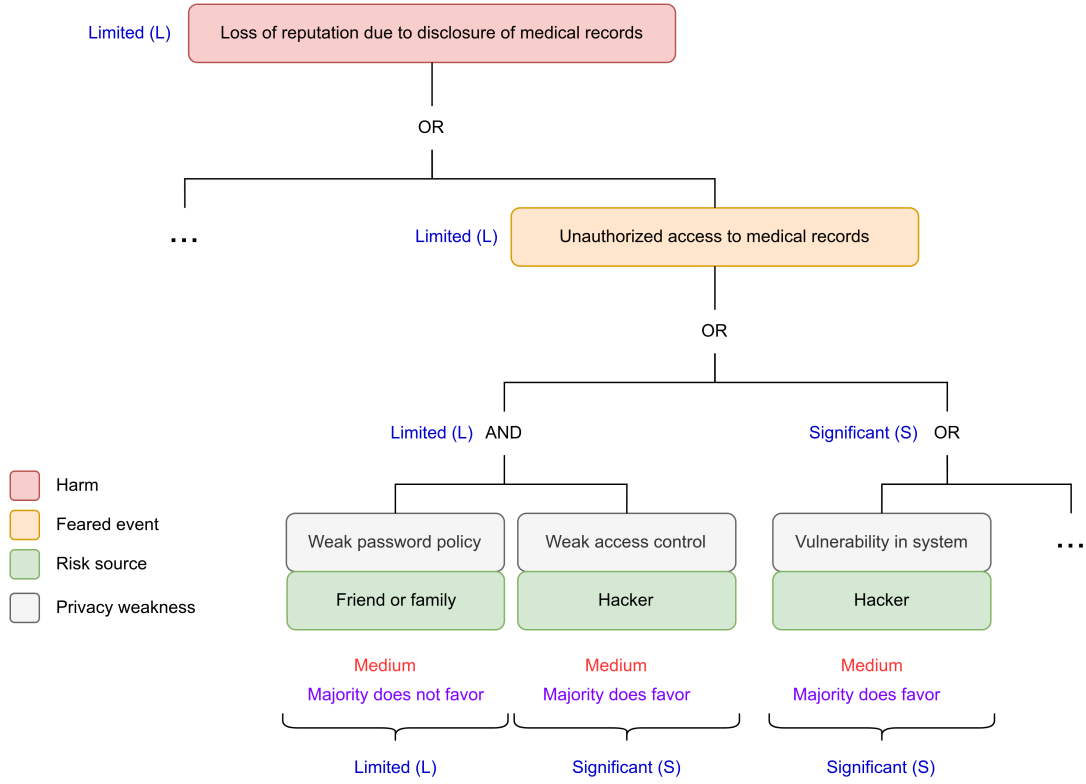


Figure 6: Harm tree with computed likelihood.

3 Privacy Harms in an Example of a Medical Breach

In this section we will examine a real world example of a medical privacy breach. First, we will quickly introduce the case. Then, we will identify the privacy harms based on PRIAM, leading to a brief discussion of the results. In consideration of the scope of this report we will not provide a harm tree and risk calculation for the example, as it describes a specific, already occurred *feared event*.

3.1 Scenario

UCLA Health, the health system of the University of California, Los Angeles (UCLA), suffered a data breach in 2015, compromising sensitive personal data of approximately 4.5 million patients. In October 2014 UCLA Health started an investigation of suspicious network traffic, which did not appear to have malicious potential. However, in May 2015 a cyberattack involving the compromise of sensitive patient information was confirmed by the officials and affected patients were informed by the organization. The data compromised in the UCLA Health data breach included personal data, as defined by the GDPR [4, Article 4(1)], such as names, addresses, dates of birth, Social Security and medical record numbers, Medicare or health plan IDs, and medical information.[5]

3.2 Privacy Harms

We will now describe the *privacy harms* for the presented scenario, based on the PRIAM model[1, Section 3.7].

Considering the scope and circumstances of the UCLA Health breach, the following examples for categories of *privacy harms* can be observed:

- *Physical harms*: A patient may be subject to stalking due to their address being leaked or receive wrong medical treatment as the consequence of the compromise of their medical data
- *Mental or psychological harms*: A patient fears misuse of their data, e.g. for identity theft, or is disadvantaged in an application due to a medical condition being disclosed
- *Financial harms*: A patient has to pay a higher health insurance premium for their alleged sedentary lifestyle inferred from medical data, or have to defend them self against identity theft
- *Harms to dignity or reputation*: Disclosure of intimate personal habits or unhealthy lifestyle may cause a patient embarrassment

Next, attributes in the form of *victim* and *intensity* can be assigned to the harms described in the categories of harms. Both attributes are measured as either *Low*, *Medium*, or *High*, depending on how many individuals are effected for the *victim* attribute, and the consequences, as well as the duration and reversibility of those consequences for the *intensity* attribute. The *severity* of the harm is then evaluated as the multiplication of both attributes. An exemplary result for the given scenario can be seen in Table 1. It will be discussed further in the next section. For the complete description of the scale used, please refer to [1, Section 3.7.1].

Harm	Example of event	Categories	Victims	Intensity	Severity
H.1	Stalking	Physical	Low	Medium	Limited
H.2	Identity theft	Psychological, financial	Low	High	Significant
H.3	Increased health insurance premium	Financial	Medium	High	Maximum
H.4	Disclosure of intimate personal habits	Harm to dignity, Psychological	Low	High	Significant
H.5	Wrong medical treatment	Physical	Low	High	Significant
H.6	Denial of Job	Psychological, Financial	Low	High	Significant

Table 1: Examples of harms of the UCLA Health breach and their attributes

3.3 Discussion

First, we should take a look at the underlying *feared event* and its relevance, considering a medical data breach. A *feared event* in PRIAM consists of a category, defined by privacy weaknesses, and the attributes *scope* and *irreversibility* [1, Section 3.6]. In the context of a medical breach, PRIAM can be extended to fit the specific needs, as proposed by Wairimu and Fritsch [6]. This adopted version provides us with the category of hacking/IT incidents for our *feared event*. Further, the *scope* is evaluated as *High*, due to the large number of affected patients, and the irreversibility is *High* as well, as disclosed data can not be undisclosed again.

In Table 1, we can observe that the *victim* attribute is most often estimated as *Low*, while the *intensity* is almost always scaled as *High*. One factor for the *intensity* evaluation is the *High irreversibility* of the *feared event* that applies to the *privacy harms* in this case as well. This leads to the *severity* of each harm being almost exclusively rated as either *Significant* or *Maximum*. We can deduce that *privacy harms* from a medical breach, while mostly only impacting a single individual, are of huge consequences for the affected individual. However, the *High scale* of the *feared event* in this incident must be considered during assesment.

Finally, we can take a look at the relative impact of each category of *privacy harm* for our *feared event*, by assigning numerical values to the *severity*, as shown in [6]. The results can be seen in Table 2, with the average severity score being build for categories with multiple *privacy harms*. It shows that the financial aspect is impacted the most for the UCLA Health breach.

Category	Harms	Severity	Avg Severity Score
Physical	H.1, H.5	Limited, Significant	2.5
Psychological	H.2, H.4, H.6	Significant, Significant, Significant	3
Harm to dignity	H.4	Significant	3
Financial	H.2, H.3, H.6	Significant, Maximum, Significant	4

Table 2: Relative impact of categories of privacy harms in the UCLA Health breach

4 Conclusion

In this report we have provided a brief overview of the PRIAM methodology. Additionally we took a more detailed look at *privacy harms* in the context of a medical breach. For that purpose we presented a case study for the UCLA Health breach. The results of the study have shown that PRIAM can be applied to medical breaches to get a meaningful understanding of the consequences and gravity of *privacy harms*. We have shown further, that the approach can be extended to get relative information about the impact of different categories of *privacy harms* in medical breaches.

References

- [1] Sourya Joyee De and Daniel Le Métayer. *PRIAM: A Privacy Risk Analysis Methodology*. Research Report RR-8876. Inria - Research Centre Grenoble – Rhône-Alpes, Apr. 2016. URL: <https://hal.inria.fr/hal-01302541>.
- [2] Directorate-General for Energy. *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems v. 2*. Accessed on 24-10-22. Sept. 2018. URL: https://energy.ec.europa.eu/system/files/2018-09/dpia_for_publication_2018_0.pdf.
- [3] *Privacy Impact Assessment for RFID Applications*. Accessed on 24-10-22. Jan. 2011. URL: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy-Impact-Assessment-Guideline-Langfassung.pdf?blob=publicationFile>.
- [4] *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. OJ L 119, 4.5.2016, p. 1–88.
- [5] Elizabeth Snell. *UCLA Health Data Breach Affects 4.5M Patients*. Ed. by healthitsecurity.com. Accessed on 24-10-22. July 2015. URL: <https://healthitsecurity.com/news/ucla-health-data-breach-affects-4.5m-patients>.
- [6] Samuel Wairimu and Lothar Fritsch. “Modelling privacy harms of compromised personal medical data-beyond data breach”. In: *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 2022, pp. 1–9.