Modelling privacy harms of compromised personal medical data - beyond data breach

Samuel Wairimu
samuel.wairimu@kau.se
Karlstad University
Karlstad, Sweden

Lothar Fritsch
lothar.fritsch@oslomet.no
Oslo Metropolitan University
Oslo, Norway

ABSTRACT

What harms and consequences do patients experience after a medical data breach? This article aims at the improvement of privacy impact analysis for data breaches that involve personal medical data. The article has two major findings. First, scientific literature does not mention consequences and harms to the data subjects when discussing data breaches in the healthcare sector. For conceptualizing actual documented harm, we had to search court rulings and popular press articles instead. We present the findings of our search for empirically founded harms in the first part of the article. Second, we present a modified PRIAM assessment method with the goal of better assessment of harms and consequences of such data breaches for the patient/employee data subject in healthcare. We split the risk assessment into parallel categories of assessment rather than calculating a single risk score. In addition, we quantify the original PRIAM categories into a calculus for risk assessment. The article presents our modified PRIAM which is the result of these modifications.

Our overall contribution is the collection of actual harms and consequences of e-health data breaches that complement the overly theoretical discussion in publications. With our operationalization of PRIAM and by providing a catalog of real harms examples, we focus privacy impact assessment on actual harms to persons.

CCS CONCEPTS

• **Security and privacy → Privacy protections**.

KEYWORDS

privacy, data breach, personal health information, consequences, risk assessment, harms, privacy impact

ACM Reference Format:
Samuel Wairimu and Lothar Fritsch. 2022. Modelling privacy harms of compromised personal medical data - beyond data breach. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3538969.3544462

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3544462

1 INTRODUCTION

The healthcare sector has been highly transformed through the application of digital health technologies that have opened vast opportunities for both patients and healthcare professionals alike. For instance, a patient can be monitored remotely with the aim of improving efficiency and increasing the quality of care. While this is the case, these technologies tend to collect extensive patient health data, for example, through mHealth devices [Kotz 2011], which are later processed, and shared for various purposes within the healthcare setting as Electronic Health Records (EHRs). These activities, which involve the collection, processing of data, and sharing, as discussed by [Solove 2006], lead to privacy invasion of data subjects (in this case patients).

In recent years, the healthcare sector has become a treasure trove for a number of cyber-attackers [Wairimu 2021]. One of the reasons, other than lagging behind other sectors in terms of cybersecurity [Kruse et al. 2017], is the rich and vast patient data. Fundamentally, this data contains personal health information (PHI) and personal identifiable information (PII) (such as name, date of birth (D.O.B), and social security numbers), which are considered valuable on the Dark web. For example, the price per unit of a small quantity of patient information containing PII could go for $3, but the price increases to $250 if it contains details such as "Doctor Fullz", that is, full information that could be used by an attacker to impersonate a real doctor for the purposes of creating false insurance claims[1]. Hence, driven by motivations such as financial gain, attacks within the healthcare sector have led to successful data breaches which affect thousands, if not millions of patients. In fact, it is shown that the frequency of data breaches and the volume of disclosed data within the sector is increasing at an alarming rate [Seh et al. 2020]; this can be evidenced in the HIPAA journal which illustrates some of the massive healthcare data breaches that were reported in the first month of 2021[2].

In general, cyber-attacks that lead to data breaches within the healthcare sector not only result in negative consequences against healthcare organisations (e.g., the financial burden that a healthcare organisation incurs after a data breach [Bhuyan et al. 2020]), but also on patients (e.g., in the case of a medical identity theft where an attacker can use the information for financial gain or treatment). However, according to Williams and Hossack [Williams and Hossack 2013] *"while people comprehend the outcome of the potential risks to the financial information, they are less aware of the risks of*

[1]Orange cyber defense: Follow-up study: Data breaches in the health sector, 2020, https://orangecyberdefense.com/global/blog/healthcare/follow-up-study-data-breaches-in-the-health-sector/, Accessed 21.03.2022
[2]HIPPA Journal : January 2021 Healthcare Data Breach Report, 2021, https://www.hipaajournal.com/january-2021-healthcare-data-breach-report/, Accessed 21.03.2022

unauthorised access to the health data and the uses that can be made of their health information". This could be attributed to the fact that the impact of privacy on a patient as a result of a healthcare data breach is mostly abstract, with only a few analysis methods targeting consumers in order to communicate privacy risks, such as in [Hatamian et al. 2019]. Nevertheless, it is argued that even though such vast amounts of patient data are exposed, there never lacks a small amount of health data (especially personal health data) that can be exploited and eventually lead to a negative impact[3].

Research published concerning cyber-attacks and data breaches within the healthcare sector is plenty; nonetheless, *only a few publications highlight the impact of privacy breaches* on a patient with regard to their personal health data. Hence, we aim to uncover key findings and address this research gap. To achieve this, we review published literature and media sources that discuss the privacy impact of breached personal health data. Based on the compiled evidence of health breach impacts and consequences, we enhance the Privacy Risk Analysis Methodology (PRIAM) for the purpose of anticipating patient impact following health data breaches. In order to achieve this, we aimed at answering the following research questions:

(1) What are the documented privacy impacts in regards to personal health information and harms to data subjects in the scientific literature?
(2) What kinds of privacy impacts on patients are documented in media channels?
(3) How can these impacts be quantified or evaluated and integrated into a risk assessment or impact analysis process?

1.1 Contributions

The key contributions of this paper are:

(1) Going beyond the data breach. We set to survey the effects of a cyber-attack that materialises as a data breach in the healthcare sector towards affected patients. From the literature survey, we show that there are few publications regarding this. Hence, we bridge this gap by providing, from non-scientific sources, the impact on the privacy of patients post-breach.
(2) An analysis of the impact on privacy by proposing an impact assessment model. Based on the effects of the data breach on the patient, the model aims at evaluating the impact on the privacy of patients by building upon PRIAM. The model aims at evaluating the impact on privacy, in this case, privacy harms, by evaluating each in isolation to show the level of impact.

In general, our research shows that while data exists showing the impact on privacy the of patients, there are few publications in the scientific journals showing this. At the same time, we illustrate that the model built from PRIAM, when applied in the cases of medical data breach consequences, can estimate privacy harms in several categories.

[3]ProPublica, DEc. 2015: Small-Scale Violations of Medical Privacy Often Cause the Most Harm, https://www.propublica.org/article/small-scale-violations-of-medical-privacy-often-cause-the-most-harm, Accessed 21.02.2021

1.2 Structure of the Paper

The rest of the paper is organized as follows: Section 2 discusses the literature search for evidence. Section 3 will provide an overview of the PRIAM assessment methodology for privacy consequences and will elaborate on how it can be operationalized on medical privacy impact assessment through a modification based on our findings from section 2. Section 4 provides the conclusion and an outlook for further work.

2 BACKGROUND SEARCH FOR EVIDENCE OF IMPACT

This section presents the background of the breach's impact on patient data. Despite extensive research and empirical evidence on cyber-attacks and data breaches in the healthcare sector, there is a limited number of scientific publications that explore or mention the privacy impact or consequences of breached PHI and PII.

2.1 Scientific Literature Survey

Table 1: Papers found in the literature survey that mention either privacy impact, consequences or privacy risk in the context of breached medical data.

Author	Year	Objective	Comments
O'Neill, Dexter and Zhang [O'Neill et al. 2016]	2016	Investigates privacy implications of posting or sharing unprotected health information (Data from anesthesia study).	Risk to patient privacy, safety and data security.
Dapaah and Senah [Dapaah and Senah 2016]	2016	Discusses privacy and confidentiality in healthcare with relation to sero-positive patients.	Patient privacy and safety.
Walsh et al [Walsh et al. 2018]	2018	Discusses privacy risks in sharing clinical research data (psychological and psychiatric data).	Risk to patient privacy and safety.
Shen et al [Shen et al. 2019]	2019	Interviews on how patients view the privacy of mental health information exchange	Patient privacy and safety
Veliz [Véliz 2020]	2020	Discusses privacy, personal responsibility, and data rights in medical settings	Patient privacy, safety and data security
Couce-Vieira, Insua and Kosgodagan [Couce-Vieira et al. 2020]	2020	Assessing and forecasting potential impacts of cyberthreats in organisations	Risks, Harm to people, impacts and security

To search and identify literature, the following search terms were used across a number of scientific databases, i.e., IEEE Xplore[4], PubMed[5], Sage[6], Wileys[7] and Springer[8]: ***(privacy impact OR consequences OR risks OR effects OR harm) AND (privacy) AND (healthcare OR hospitals) AND (patient data OR personal health information OR personal health data) AND (breach).*** We restricted our search to the last five years so as to yield recent results. We inspected the primary results of the search for a description of the actual consequences of data breaches for patients. While most of the papers discuss data breaches, they fail to mention harms or consequences. Only a few scientific articles actually mentioned specific examples of harm to patients, or systematic categorization

[4]https://ieeexplore.ieee.org/Xplore/home.jsp
[5]https://pubmed.ncbi.nlm.nih.gov/
[6]https://journals.sagepub.com/
[7]https://www.wiley.com/en-us
[8]https://link.springer.com/

of such harms. Table 1 displays the results of the literature survey that we conducted, while Table 2 shows the classification of the medical breach consequences derived from the papers identified in Table 1.

Table 2: Classification of medical breach consequences.

Author	Type of evidence	Impact
O'Neill, Dexter and Zhang [O'Neill et al. 2016]	Hypothetical	Hypothetical press leakage
Dapaah and Senah [Dapaah and Senah 2016]	Anecdotal	Patient stigmatization
Walsh et al [Walsh et al. 2018]	Hypothetical	Embarrassment, Stigmatization, Discrimination, Loss of job
Shen et al [Shen et al. 2019]	Interviews	Stigmatization, Loss of control, Loss of job
Veliz [Véliz 2020]	Anecdotal, Hypothetical	Loss of job, Discrimination, Financial loss, Blackmail
Couce-Vieira, Insua and Kosgodagan [Couce-Vieira et al. 2020]	Anecdotal, Hypothetical	Cyberbullying, Harm to personal rights

In their paper, O'Neill, Dexter, and Zhang [O'Neill et al. 2016] provide both hypothetical and real scenarios. Although the real scenarios are not directly related to patients and their health data, they present a case study and a hypothetical scenario where unprotected health information, for instance, hospital name and surgical codes could be used to re-identify a patient (if accessed by an adversary either maliciously or non-maliciously). While they are keen to mention the risks of re-identification of patients' sensitive information, such as the exposure of potentially harmful information, they do not mention the impact of privacy on patients.

Dapaah and Senah [Dapaah and Senah 2016] address the issue of breach of privacy where healthcare professionals in a clinical setting tend to disclose the HIV status of patients either intentionally (by disclosing the status of a patient to a relative or spouse deliberately) or unintentionally. The disclosure of such sensitive information always has an impact on the affected patient. For example, the authors of the paper mention an instance where a patient could get divorced (they provide a real impact for this, where a patient was divorced after their status was purposely disclosed to their partner), discriminated against, lose a job, or even rejected due to the disclosure of their status.

Work by Walsh and colleagues [Walsh et al. 2018] assesses the risks to privacy when research data concerning the mental health of patients is disseminated within a mental clinic. They discuss some of the consequences that could occur if a patient is re-identified from the collected data. These consequences are: embarrassment, discrimination, and stigmatization of a patient.

A study conducted by Shen et al [Shen et al. 2019] examines the point of view of patients on risks concerning the dissemination of their mental health information within a clinic. Participants of the study highlighted their risks, and while they recognised the existence of malicious actors, this did not concern them much as they acknowledged other risks. For example, certain employers gain access to PHI in unauthorised manner. One of the participant's provided a negative impact where a boss discriminated against them from a job role based on the PHI that they obtained from an insurance company.

Veliz [Véliz 2020] identifies and discusses potential harms that would take place as a result of a breached personal medical data. Some of these harms are: job discrimination based on PHI disclosed, price discrimination in the context of an insurance company, and identity theft.

Couce-Vieira, Insua, and Kosgodagan [Couce-Vieira et al. 2020] discuss the impact of cyber threats in organisations and proposes a forecasting model to assess the impact of these threats. They discuss objectives, which, among others, include harm to people. They point out harms such as mental and physical health, harm to personal rights, financial harm, and fatalities (by tampering with medical devices). Furthermore, they construct a scale that ranks the levels of mental and physical impacts (under harm to people) built upon some scoring systems (e.g., GAF (Global Assessment of Functioning), ISS (Injury Severity Score)).

2.2 Documented cases of breach consequences in media

From the above survey, it can be deduced that there is a very limited number of publications that directly address the privacy impact of breached personal health data. Despite this, a number of non-scientific published sources, for example, reports, lawsuits, and news media, highlight the impact on privacy when a patient's data is accessed maliciously or accidentally, with consequences. In order to assess and classify such consequences, we reviewed media and internet publications for such descriptions.

To identify sources that could yield information about the impact on the privacy of patients, the following search techniques were applied:

- Search by topic - We searched for a number of topics using the Google search engine. These topics are:
  consequences of breached medical data to patients, stalking of patients after a medical data breach, disclosure of medical data and its effects on patients, cases of patients asked for ransom based on breached medical data, death of patient as a result of breached medical data, embarrassment to patients after disclosure of personal health information, and lawsuits and fines as a result of impact to privacy with regards to breached medical.
- Search by Phrases - We also searched phrases to find more articles on whether there have been reported cases concerning the impact on the privacy of breached medical data against patients. To search, the following phrases were applied:
  "consequences", "breached medical data", "personal health information", "privacy impact", "effects", "lawsuits".

We used the Google search engine with the aim of finding and yielding results that indicated harms and consequences experienced by patients. Findings are listed in the footnotes below and in Table 3.

Table 3 illustrates a number of cases and impacts derived from the identified sources. To complement these, we added the case of

Table 3: Selected cases of privacy impact of breached medical data.

Case	Impact	Type of Breach	Location of Breached Information
Medical records of a Florida woman were disclosed by a nurse thus revealing her long secret[9](Real case).	Fear, Embarrassment	Unauthorised Access/Disclosure (Internal)	EHRs
The case of Hinchy v. Walgreen Co. - Disclosure of patient's prescription history that led to criticism from her ex-boyfriend[10](Real case)	Emotional Distress	Unauthorised Access/Disclosure (Internal)	Prescription records
Medical data from the World Anti-Doping Agency concerning athletes disclosed[11](Real case).	Possible cause of fear/distress	Hacking/IT Incident	EHRs
Disclosure of patient's sensitive status on social media[12](Real case).	Embarrassment	Unauthorised Access/Disclosure (Internal)	Medical Records
Individual targeted for medical identity theft - bills totaled to almost 20,000 US Dollars[13](Real case)	Financial strain, Distress	Stolen Information	ID and Medical Records
Medical records of a woman accessed and disclosed by ex-partner in an unauthorised manner[14](Real case)	Anxiety, Stress	Unauthorised Access/Disclosure (Internal)	EHRs
A NHS staff member disclosed personal medical data regarding her sister-in-law to the family members[15](Real case)	Anxiety, Stress, Trauma - that led to psychological effects and medication, and threats	Unauthorised Access/Disclosure (Internal)	EHRs
A patient's HIV status, including his PII remained in the public open record for at least six months prior to being sealed after a lawsuit filed by collections attorney on behalf of a healthcare provider seeking payment for an unpaid debt[16](Real case).	Emotional distress, Embarrassment	Disclosure (Internal)	Paper/Films
Doctor provides an investigator with full medical records of a patient to dig dirt on him after a complaint to the Medical Board of California[17](Real case).	Vengeance	Disclosure (Internal)	Paper/Films
Patients, including a prominent individual in Finland, received emails demanding ransom after a breach of psychotherapy records[18](Real case).	Blackmail, Distress	Hacking/IT Incident	EHRs
A case in which doctors' breached the privacy of one of their colleagues after accessing into his medical records[19](Real case).	Stigmatisation	Unauthorised Access/Disclosure (Internal)	EHRs
Women targeted after a data breach at the University Hospital Crosshouse[20](Real case).	Stalking	Hacking/IT Incident	EHRs
Exposure of patient data led to the disclosure that an influential person in politics was using an ICD (Implantable Cardioverter-Defibrillator). An attacker gained access to the device and manipulated the data, which led to a cardiac arrhythmia (Demonstrated [Rios and Butts 2017] and Hypothetical).	Death	Hacking/IT Incident	EHRs

the hacked heart pacemaker, which has been shown to be possible in laboratory conditions.

[9]Tampa Bay Times: Medical records breach at Tampa General, USF exposes woman's secrets, June 2013, https://www.tampabay.com/news/health/medical-records-breach-at-tampa-general-usf-exposes-womans-secrets/2129083/, Accessed: 21.03.2022

[10]Breazeale, Sachse & Wilson, L.L.P., https://www.bswllp.com/the-intersection-of-hipaa-and-negligence-pharmacists-violation-cost-walgreens-144-million, Accessed: 21.03.2022

[11]BBC News: Wiggins and Froome medical records released by 'Russian hackers', September 2016, https://www.bbc.com/news/world-37369705, Accessed: 21.03.2022

3 PRIAM: EXTENSION OF A METHOD FOR PRIVACY HARMS ASSESSMENT

The privacy of patients and the protection of their health data is a fundamental right that is essential in the healthcare sector. While it has many facets, complex and governed by laws, privacy is crucial when it comes to safeguarding the data subjects; hence, when conducting a privacy risk analysis including patient impact, these aspects need to be considered; in particular the concept of privacy harm. For this purpose, we first introduce the PRIAM method. Then, we show how we adapted PRIAM in order to improve the health data breach impact assessment.

3.1 Introduction of PRIAM

PRIAM [De and Le Métayer 2016] is a methodology for a privacy impact assessment that focuses on harm to individuals. It constitutes seven components that are vital for a privacy risk analysis in the information gathering phase. However, of focus in this research is data, feared events and privacy harms components that will be used at a later stage to construct a model for impact assessment. Furthermore, patient data is an important element in the healthcare sector; thus during privacy risk analysis it is essential to determine attributes and categories of the data that will be essential in identifying privacy flaws and feared events [De and Le Métayer 2016].

3.2 Data

When performing a privacy risk analysis, the category of personal data being processed within a particular setting needs to be factored in. One of the categories of personal data is the health data that contains a patient's PHI and PII. Under this, there are a number of attributes that need to be considered during the analysis [De and Le Métayer 2016]. These are:

- **The nature of data being processed, that is, its sensitivity**: Health data is legally considered as a special category

[12]NPR Morning edition: Small Violations Of Medical Privacy Can Hurt Patients And Erode Trust, December 2015, https://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust , Accessed: 21.03.2022

[13]CBS News: Hackers are stealing millions of medical records – and selling them on the dark web, February 2019, https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/, Accessed: 17.01.2022

[14]HayesConnor Soclictors web page: Woman has her medical records unlawfully accessed by her ex, https://www.hayesconnor.co.uk/news-and-resources/case-study/woman-has-her-medical-records-unlawfully-accessed-by-her-ex/, Accessed: 21.03.2022

[15]HayesConnor Solicitors web page: NHS family member shared confidential medical information, https://www.hayesconnor.co.uk/news-and-resources/case-study/nhs-family-member-shared-confidential-medical-information/, Accessed: 21.03.2022

[16]See Eggeson, 2021.

[17]See NPR, 2021.

[18]The Guardian: 'Shocking' hack of psychotherapy records in Finland affects thousands, October 2020, https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland, Accessed: 21.03.2022

[19]NZ Herald: Breach of doctor's privacy by colleagues condemned by medical authorities, unions, July 2020, https://www.nzherald.co.nz/nz/breach-of-doctors-privacy-by-colleagues-condemned-by-medical-authorities-unions/US35AYFBYZRX6DZKWUWKRRE6AE/, Accessed: 21.03.2022

[20]Cumnock Chronicle: 'Stalker' rap after hospital data breach, December 2018, https://www.cumnockchronicle.com/news/17310994.stalker-rap-hospital-data-breach/, Accessed: 21.03.2022

of personal data i.e., sensitive, under GDPR (Art. 9) and other privacy laws, for instance, the HIPAA Privacy Rule[21].

- **Format of the data**: This can be either in terms of form, precision and volume. Under form, health data collected could be pre-processed or raw. With regards to precision, a patient could disclose their date of birth, address, name, etc, depending on what is being requested. The volume depicts the amount of health data collected over a period of time.
- **Context:** This includes, the source of data (which can either be directly from the patient, indirect (implicit) disclosure, or third party disclosure (for example through family or friends)), the purpose of the data and the period of retention.
- **Control over data:** This includes visibility - people who are authorised to access the data and probably read it, and intervenability, which allows a patient to have control over their data through the data subject rights.

The above attributes have a strong-attribute category link with feared events. That is, the exploitation of these attributes under the data category has a higher probability of causing a privacy harm.

3.3 Privacy Harms

PRIAM identifies privacy harms to data subjects in five categories [De and Le Métayer 2016]:

(1) Physical, (2) Financial (3) Psychological, (4) Harms to dignity (5) Societal

Under each category falls the attributes of *victims* (in this case patients) and the *intensity* of harm, which are both expressed as low, medium, and high. The affected victims' sum is three: LOW - an individual, MEDIUM - a particular set of patients, HIGH - the whole population [De and Le Métayer 2016]. On the other hand, the intensity is evaluated based on numerous consequences experienced by the victim as a result of the harm, that is, *irreversibility*, *duration* of exposure, and *extent of damage*.

Fig 1 illustrates how feared events (with its respective attributes) result in harms that lead to consequences that impact victims (patients), with differing scales and duration.

Evaluating Privacy Harms: In a healthcare organisation, a data breach that occurs as a result of intentional or unintentional unauthorised access to data results in negative consequences as indicated in Table 3. Hence, by mapping the cases identified in Table 3 against the PRIAM privacy harms categories, we construct a matrix to evaluate impact assessment as illustrated in Table 4.

3.4 Extension of PRIAM for Health Data Breach Impact

In this section, we will present our modification of the PRIAM method. We pursue two goals. First, we aim at including the specificities of medical breaches and their consequences in the analysis process, which we achieve by adapting concepts such as feared events, and by the provision of examples for classifying event scales. Second, we aim at calculating the overall impact through quantitative risk assessment. Therefore, we introduce a calculus that will produce an overall impact assessment score.

[21] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html, Accessed 21.03.2022

Table 4: Harms in the healthcare context in relation to their PRIAM attributes.

Harm	PRIAM Category of harm	Victims	Intensity	Severity
Disclosure of patient's sensitive data to the public	Psychological, dignity and reputation	Low	High	Significant
Individual left to pay bills after a medical identity theft	Financial	Low	Medium	Maximum
Athletes medical data exposed from the World Anti-Doping Agency	Psychological, Dignity and Reputation	Medium	Low	Limited
Extortion and blackmail of patients whose mental health data got exposed in Finland.	Psychological, Financial, Dignity and Reputation	Medium	Medium	Significant
Women targeted after healthcare data breach from the University Hospital Crosshouse.	Physical	Medium	Low	Limited

3.4.1 Feared Events in the Healthcare Context. Taking into consideration the data and the attributes highlighted above, one can identify the categories of *feared events* within a particular healthcare setting. According to De & Le Métayer [De and Le Métayer 2016], feared events occur as a result of taking advantage of one or several privacy flaws, which eventually lead to privacy harms for the affected patients (feared events and privacy harms have a category-category link) [De and Le Métayer 2016]. Hence, when performing an analysis of feared events in the healthcare context, the following must be considered:

- **Hacking/IT incidents** (Unauthorised access to health data - External) - Based on its nature and the precision of patient health data that is normally collected, PHI has become a preferred target for malicious hackers [Chernyshev et al. 2019]. This category can also lead to the modification of patient data if accessed with malicious intent.
- **Unauthorised disclosure** (Internal) - The attribute of visibility allows authorised individuals to access patients' data whenever needed. However, there are cases where insiders (e.g., an employee or trainee) access and disclose data either accidentally, based on curiosity [Van Deursen et al. 2013] or for malicious purposes. According to Johnson [Johnson 2009], this causes data hemorrhages, which leads to negative consequences for the affected patients.
- **Excessive collection of health data** through medical devices - As discussed, digital technologies offer an advantage when it comes to monitoring the health of a patient remotely or for self-management. However, these devices collect excessive PHI frequently over a certain time interval [Kotz 2011]. Fundamentally, this goes against the principle of data minimisation as highlighted in Article 5 of the GDPR.
- **Using health data for unauthorised purposes** - For instance, when an authority decides to use centrally collected health data to re-identify users who are infected with COVID-19 [Castelluccia et al. 2020; Hatamian et al. 2021]. This also undermines the principle of purpose limitation as indicated under the principles related to the processing of personal data in the GDPR.

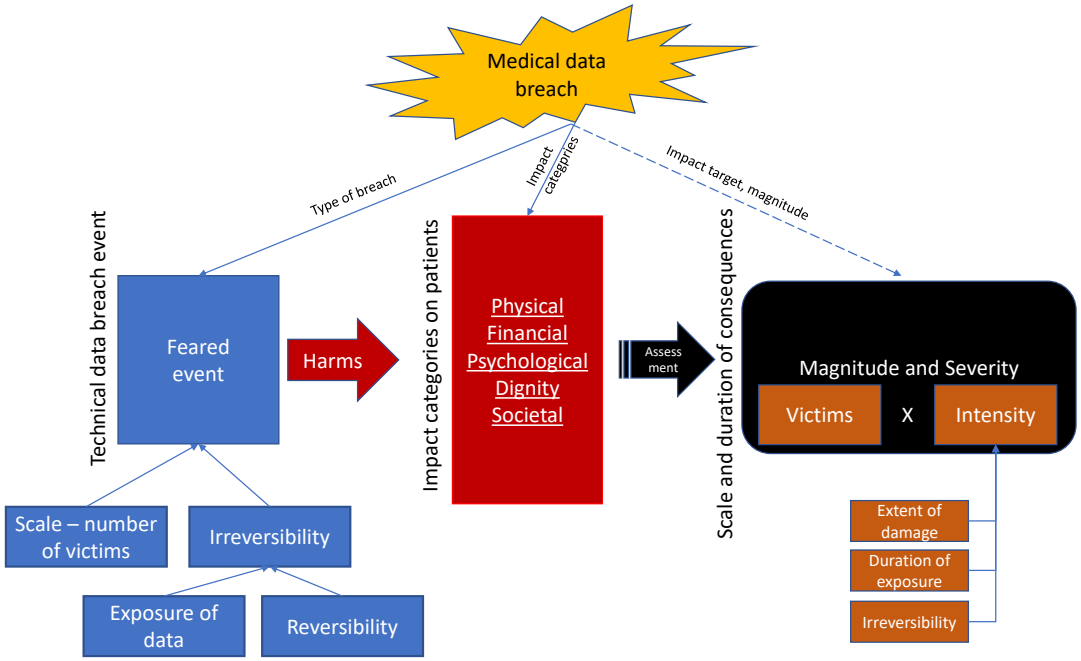

Figure 1: PRIAM approach of privacy impact assessment.

- **The use of incorrect health data** - [Cohen 2015] identifies the risk of treating a real patient with medical records that have been compromised by an attacker for medical identity theft. This might cause the patient to get the wrong prescription or misdiagnosis at a later time. As such, patient data needs to be rectified as soon as inaccuracies are identified as highlighted under Article 5 of the GDPR.
- **Storing health data more than is required** - this results in the storage of incorrect PHI and PII or poor security measures which would result in privacy issues. Furthermore, storing personal data more than is needed undermines the principle of storage limitation under GDPR.

This component, just like data, has its own attributes that need to be factored into events: *Scale* and *Irreversibility*. To evaluate the attribute *scale*, we assess the number of potential patients whose medical data is concerned. Hence, following the PRIAM, we place these under high, medium, and low. The attribute of *irreversibility*, can be evaluated by how difficult a feared event can be reversed. Hence, to evaluate this attribute, two factors are considered: the magnitude of patient data disclosed as a result of an event disclosure, and the technical difficulty to undo the impact of the listed events [De and Le Métayer 2016]. Hence, coupling the feared events, with the scenarios identified in Table 3, the scale and irreversibility can be evaluated as shown in Table 5.

3.4.2 Scale, Victims and Irreversibility. In order to come forth with an evaluation of privacy harms specific to the medical sector, and using PRIAM in order to calculate the impact of compromised healthcare data, we adopt the following classification in order to map potential privacy impact:

Table 5: Examples for Feared Events from documented cases within the healthcare context in relation to their PRIAM attributes.

Feared Events	Case	Scale	Irreversibility
Hacking/IT Incident (Unauthorised access to health data - External)	Psychotherapy records of patients, including that of a prominent person exposed in Finland	Medium	High.
Unauthorised Disclosure of personal medical data (Internal)	Exposure of patient's sensitive data to public/Exposure of PHI to family members	Low	High.
Using health data for unauthorised purposes	Use of collected patients data for other purposes than one specified.	High	Medium.
Using inaccurate patient health data	Possibility of treating the right patient with wrong medical data derived from a medical identify thief	Low	High.

Scale: One patient (low) - limited group of patients (medium) - large group of patients (high).
Victims: An individual patient (low) - a specific group of patients (medium) - society (high).
Irreversibility: Low (easily reversible) - medium (slightly reversible) - high (Not easily reversible).

3.4.3 Adding Risk Calculation. While in the PRIAM approach the affected categories of harm get listed together for one assessment, we propose to calculate harm individually for each category. The motivation for this addition to PRIAM is that we see very different harm potentials from a single breach in the individual harm categories, e.g. where it comes to financial reversibility (through compensatory payments) versus irreversible physical or psychological damages that come from the very same breach. Therefore, we see value in the individual assessment of each harm category.

Table 6: Evaluation of severity score.

Privacy Harms	Severity Score	Severity
Physical	4	Significant
Financial	9	Maximum
Psychological	3	Significant
Dignity	3	Significant
Societal	9	Maximum

PRIAM's classification is not fit for calculus; as such, we convert the assessments into a numerical scale. In order to capture and visualize specific impact, the parameters will have to get quantified. We therefore interpret PRIAM's scale of *low - medium - high* as numerical *1 - 2 - 3*. The result of the above calculations will be normalized on a scale of 1 to 3. As such, we calculate each privacy harm category by evaluating the attributes of victims and intensity as indicated in Figure 4 (see section A)

With regards to the severity of the affected patients, we calculate *Severity* as: $(victims * intensity)$ where *intensity* is one of {Low, Medium, High} while $victims = groupsize * intensity$, with intensity illustrated in [De and Le Métayer 2016] as:

LOW: Receipt of unsolicited mails, targeted advertising; MEDIUM: Undesirable disclosure of intimate personal condition to friends, re-scheduling of treatment, potential stalking; HIGH: Increased health insurance premium, denial of a job, undesirable disclosure of intimate personal habits to the public, the risk for mistreatment, harassment, exposure to hate crime and exclusion.

3.4.4 Making Sense of Severity Scales. According to the PRIAM document, severity is denoted as negligible, limited, significant, and maximum. Figure 2 shows a matrix that was constructed to evaluate severity - based on the matrix, the severity (shown in four colors), is a product of intensity and victims. Hence, the values derived for severity can be assigned as *1* for negligible, 2 for limited, 3 and 4 for significant, and 6 and 9 for maximum severity, as shown in Table 6.

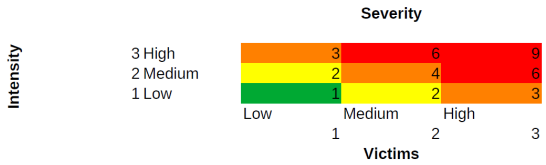

Figure 2: Assessment of severity. The severity in this case is the product of intensity and victims, which were given a numerical value of 1,2 and 3 respectively.

In order to visualize the overall contribution of each category, we visualize their share of the total severity as shown in Fig. 3. This percentage score is calculated based on Table 6.

4 CONCLUSION AND FURTHER WORK

In this paper, we investigated the question of how the actual impact of medical data breaches can be analyzed. We searched scientific literature for known models of medical data breach impact on patients, however, found only an abundance of articles that are concerned with the likelihood of a breach occurring. To collect

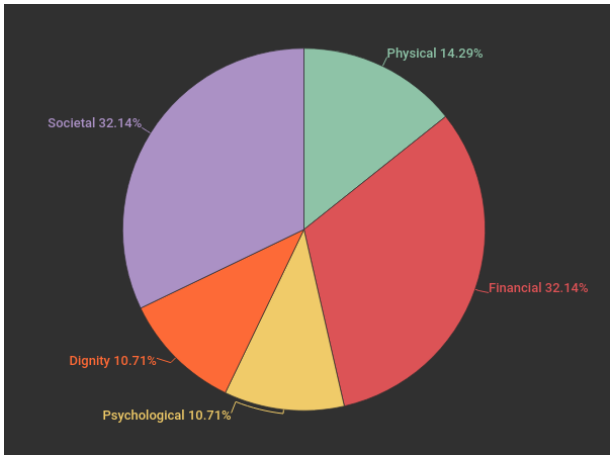

Figure 3: Severity of Privacy harms. The pie chart, calculated from Table 6, shows the relative impact of each category of privacy harm. As shown, in the event of a breach, the societal and the financial aspects would be impacted greatly.

descriptions of harms, we had to gather cases from the press, media, and other internet sources, which we compiled in a collection of examples of medical data breach consequences and harms. We established a gap in knowledge concerning actual consequences, while at the same time showing that data exists.

We operationalized harm assessment with the PRIAM approach for privacy impact assessment, which offers a detailed approach that differentiates between breach events and harms caused by a breach. We adapted PRIAM into a multifaceted analysis that illustrates different harm categories for each breach. We showed that by adding this relatively small overhead of analysis, we can achieve a better impression of the actual consequences of a medical personal data breach event. We showed that the PRIAM method can, using a classification of medical data breach consequences, estimate potential harms in several categories. Our adaption of PRIAM enables the differentiation of such harms per category.

Future work will involve two activities. A collection of case examples will be described in our adapted PRIAM notation in order to help with the analysis of potential privacy harms of medical data processing. We foresee a field study with a tool-based application of the enhanced PRIAM where we apply the methodology in clinical and medical contexts together with medical data processing and data protection experts.

ACKNOWLEDGMENTS

The work leading to this project was sponsored by the Digital Well Research project funded by Region Värmland, Sweden.

A APPENDIX

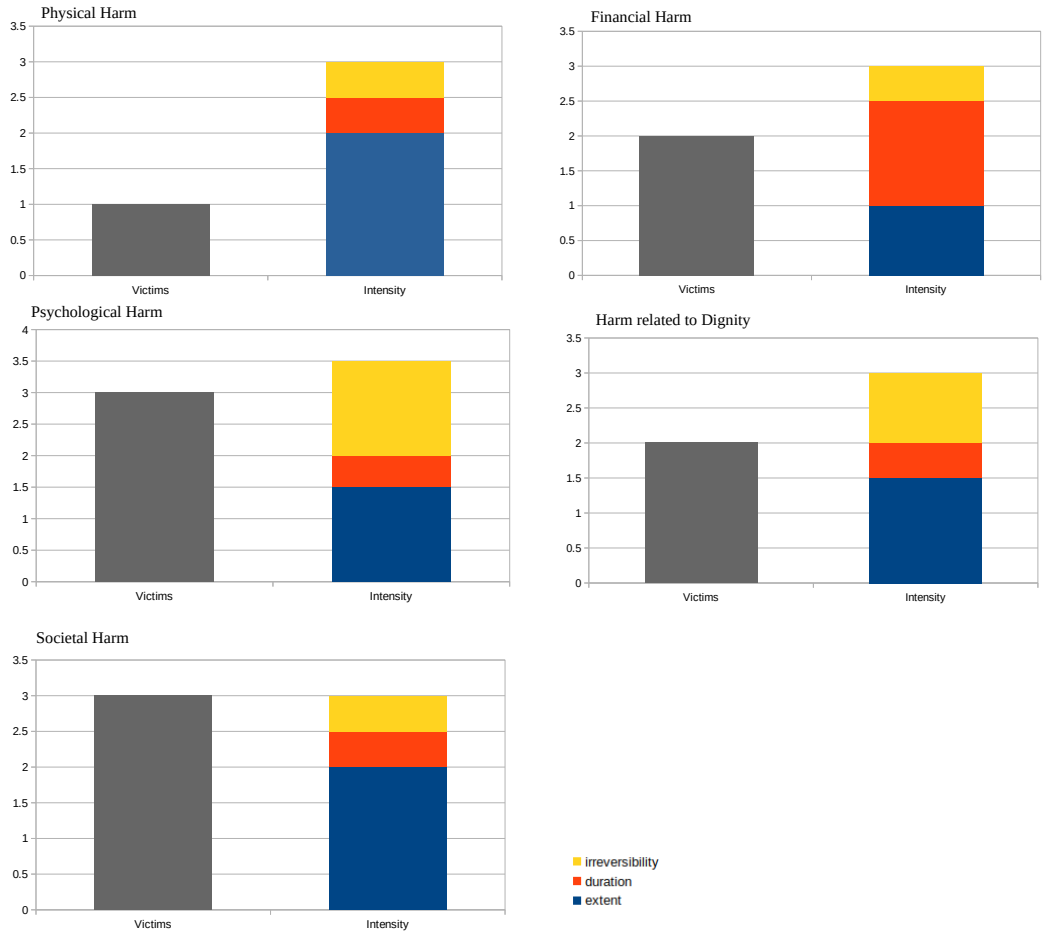

Figure 4: Illustration of privacy harms extracted from a real scenario in Table 3. The scenario: Patients in Finland received emails demanding ransom after a breach of psychotherapy records. As highlighted, while all patients within the centre suffered the same breach, it can be argued that not all shared the same harm. Under physical harm, a patient can attempt to injure themselves as a result of embarrassment. In the case of financial harm, a group of patients who received emails demanding ransom may pay not to have their data exposed. Psychological harm is caused where patients became distressed after their data was taken. Harm to dignity, where patients, might fear or get their reputation ruined. And societal harm, where the society was shattered at a general basis.

REFERENCES

Soumitra Sudip Bhuyan, Umar Y Kabir, Jessica M Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, Marian Levy, Satish Kedia, Dipankar Dasgupta, et al. 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems* 44, 5 (2020), 1–9.

Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cédric Lauradoux, Daniel Le Métayer, and Vincent Roca. 2020. ROBERT: ROBust and privacy-presERving proximity Tracing, Report hal-02611265, version 1.

Maxim Chernyshev, Sherali Zeadally, and Zubair Baig. 2019. Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems* 43, 1 (2019), 1–12.

Joshua Cohen. 2015. Medical Identify Theft - The Crime That Can Kill. *MLMIC Dateline* 14 (2015). Issue 2. https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf (Accessed: 09.03.2021).

Aitor Couce-Vieira, David Rios Insua, and Alex Kosgodagan. 2020. Assessing and forecasting cybersecurity impacts. *Decision Analysis* 17, 4 (2020), 356–374.

Jonathan Mensah Dapaah and Kodjo A Senah. 2016. HIV/AIDS clients, privacy and confidentiality; the case of two health centres in the Ashanti Region of Ghana. *BMC medical ethics* 17, 1 (2016), 1–10.

Sourya Joyee De and Daniel Le Métayer. 2016. PRIAM: A Privacy Risk Analysis Methodology. In *Data Privacy Management and Security Assurance*, Giovanni Livraga, Vicenç Torra, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri (Eds.). Springer International Publishing, Cham, 221–229.

Majid Hatamian, Nurul Momen, Lothar Fritsch, and Kai Rannenberg. 2019. A Multilateral Privacy Impact Analysis Method for Android Apps. In *Privacy Technologies and Policy*, Maurizio Naldi, Giuseppe F. Italiano, Kai Rannenberg, Manel Medina, and Athena Bourka (Eds.). Springer International Publishing, Cham, 87–106.

Majid Hatamian, Samuel Wairimu, Nurul Momen, and Lothar Fritsch. 2021. A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical Software Engineering* 26, 3 (2021), 1–51.

M Eric Johnson. 2009. Data hemorrhages in the health-care sector. In *International Conference on Financial Cryptography and Data Security*. Springer, 71–89.

David Kotz. 2011. A threat taxonomy for mHealth privacy. In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*. IEEE, 1–6.

Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and D Kyle Monticone. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 25, 1 (2017), 1–10.

Liam O'Neill, Franklin Dexter, and Nan Zhang. 2016. The risks to patient privacy from publishing data from clinical anesthesia studies. *Anesthesia & Analgesia* 122, 6 (2016), 2017–2027.

Billy Rios and Jonathan Butts. 2017. *Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies*. Technical Report. WhiteScope.

Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. 2020. Healthcare data breaches: Insights and implications. In *Healthcare*, Vol. 8. Multidisciplinary Digital Publishing Institute, 133.

Nelson Shen, Lydia Sequeira, Michelle Pannor Silver, Abigail Carter-Langford, John Strauss, and David Wiljer. 2019. Patient Privacy Perspectives on Health Information Exchange in a Mental Health Context: Qualitative Study. *JMIR mental health* 6, 11 (2019), e13306.

Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (2006), 477.

Nicole Van Deursen, William J Buchanan, and Alistair Duff. 2013. Monitoring information security risks within health care. *computers & security* 37 (2013), 31–45.

Carissa Véliz. 2020. Not the doctor's business: Privacy, personal responsibility and data rights in medical settings. *Bioethics* 34, 7 (2020), 712–718.

Samuel Wairimu. 2021. E-Health as a target in cyberwar: Expecting the worst. In *Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS)*. Academic Conferences International.

Colin G Walsh, Weiyi Xia, Muqun Li, Joshua C Denny, Paul A Harris, and Bradley A Malin. 2018. Enabling open-science initiatives in clinical psychology and psychiatry without sacrificing patients' privacy: Current practices and future challenges. *Advances in Methods and Practices in Psychological Science* 1, 1 (2018), 104–114.

Patricia AH Williams and Emma Hossack. 2013. It will never happen to us: The likelihood and impact of privacy breaches on health data in Australia.. In *Studies in Health Technology and Informatics, Volume 188: Health Informatics: Digital Health Service Delivery – The Future Is Now!* 155–161. https://doi.org/10.3233/978-1-61499-266-0-155