Cybersecurity, Data Breaches With A Focus On Trust In Dutch Healthcare Organizations

Jubilee Djan	Amine Abba	Samim Kilar	Bilal el Azrak
2108615	2108339	2086526	2099876

ABSTRACT

The increasing privacy intrusions within the Dutch health organizations has led to a decrease in trust of-people affected by data breaches. In today's world, it is crucial for health organizations to reassure the public that their personal data is secure. The long-term effects on data governance and, more broadly, on society could be negative and irreversible if the government is unable to ensure the security of personal data. According to this study, data breaches have a detrimental impact on people's confidence in health organizations' ability to protect personal information, which in turn reduces their willingness to provide the personal information that is required. The authors were able to offer suggestions for addressing these consequences after conducting interviews.

Keywords
COVID-19, Privacy Concerns, Trust, Data Breaches, Data Sharing

I. INTRODUCTION

In 2021, personal data of 6.5 million people was put up for sale in Telegram by GGD employees. There have been more than 80,000 complaints from people claiming that their data has been stolen and misused (ICAM, 2022). In the published issue, GGD confirmed that the data was stolen due to the lack of encryption. In addition, 22,000 employees had access to the data, although most of them were not authorized to access the data. At last, there was no monitoring. That is one of the reasons why GGD has been unable to act quickly and also why they don't know how much data has been stolen. Health organizations such as hospitals and organizations and screening organizations receive personal data from the Basic Registration Persons (BRP). This personal information allows them to care for patients and conduct health research. So, there is an importance to keep this information secure. Health research is valuable to society, just like privacy. Health research is undergoing a transformation due to developments in health information technology. This change made it possible to conduct studies that were previously impractical and, as a result, provide new insights into health research and disease. This is a perfect example why the development and use of data tools for pandemic control, can have potentially harmful and irreversible implications for data governance and, more generally, for society in the long term.

II. PROBLEM STATEMENT

In this paper, we seek to determine to what extent the Dutch public health authorities can enhance the trust of the citizens after a data breach. And how the public health authorities can provide transparent information about data violations to the people to regain their trust. The trust of the people has been damaged, due to the fact that health institutes were not managing the personal data as they should be. As a result of this fact, the willingness of the people to share their data with the instances, has become drastically low. The data that individuals share with the health authorities allows the health authorities to obtain, produce and analyze predictive analytics that they can use to make critical decisions. The health authorities are compelled to make critical decisions based on this information. if people are unwilling to submit the required data. This may lead to a lack of flexibility and reactivity in the face of unexpected events like the Covid-19 pandemic.

Research must be conducted to find means to reassure citizens and increase trust in order to safeguard the integrity of public data collecting and to ensure that this valuable tool is not completely withdrawn from the toolbox of public health professionals.

III. RESEARCH QUESTION

The following research question will be analyzed to examine the association between data privacy and the trust of Dutch citizens:

To what extent are the Dutch health organizations able to regain trust from the people who have been affected by any of the data breaches?

The following sub-questions support the main research question:

- What are data breaches?
- What is trust in health?

- To what extent are data breaches and trust related regarding Dutch health?
- Which aspects of data breaches have led to less trust towards Dutch health organizations?
- How big are the data breaches in the Dutch health organizations?
- What is the measured trust towards the government?

IV. METHOD

This paper is divided into two main sections: literature evaluation and data collection using interviews. These two phases are used to quantify the primary research question, the association between data privacy and the level of trust among Dutch citizens who have been affected by data breaches. Archival research is conducted to evaluate the most recent research on the subjects of data privacy and trust. Furthermore, the conceptual framework is created by literature study and is supported by the results of the interviews. We can assess the correlation between the factor's digital privacy and trust thanks to the qualitative interviews. The interview questions will be based on a study by Bill McEvily & Marco Tortoriello (2011) In which they give recommendations and review on how to measure trust. This design is slightly modified to our own paper. We use Bill McEvily & Marco Tortoriello statements as a source for questions to use during our interviews. The statements are measured and evaluated based on a 5-point likert scale. This makes it easy to award scores and assess a person's level of trust in health organizations, but also makes it particularly clear to what extent the data breaches influence the trust of Dutch citizens. As a result, both qualitative and quantitative data are collected with the intention of gaining deeper understanding of the interviewees on the one hand and demonstrating the relationship between the two variables on the other hand. Using open-ended questions as a guide, the interviews are semi-structured.

Sampling process
Due to the fact that this has been a recent topic in The Netherlands, the target population has been designated as "People who have been affected by data breaches."

The used sampling design is snowball sampling because of the difficulty to find people who want to be interviewed. The first survey respondents were drawn from the authors' (social) networks, as it was known that they had been victims of data breaches in the past. After that, the authors kept asking participants if they know other people who have been through similar situations. As a result, the authors were repeatedly put in contact with other people who belong to the target group. The information provided by the initial response is then used to select the subsequent respondents. Then, this process continues in waves for as long as necessary.

Reliability:
In this study, an acceptable Cronbach's alpha value is one of at least 0.7. The chapter results provide the scores assigned to each variable.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum V_i}{V_t}\right)$$

In this survey, pre-made scales and adopted questionnaires from other studies are employed. This study modified some of these questions to fit the setting.

Validity
The survey has been pre-tested before being deployed. All of the pre-test participants came from the authors' personal networks, and they provided comments on the length of the survey, the similarity of the questions, and any translation mistakes.

In response, one independent variable was eliminated in order to make the survey shorter. In terms of the language and wording of the questionnaire, it is advised that it should approximate the respondents' level of comprehension. If certain inquiries were misunderstood or were perceived incorrectly the question had to be rephrased (*Research Methods for Business*, z.d.). After learning about the translation issues during the pre-test, efforts were taken to improve the survey.

The anonymous nature of the interview was disclosed to respondents. It was stated in the interview's introduction that the data could not possibly be linked to an individual.

V. RELEVANCE

In this paper we focus on health organizations such as hospitals. But the findings of this paper could also be of relevance to other establishments such as: governments, banks, research organizations, tax organizations, law enforcements and other organizations. These establishments also have access to personal data from the Basic Registration Persons (BRP) (Ministerie van Algemene Zaken, 2022). and are trusted by the citizens to keep this information secure. In order to protect sensitive information, these organizations set up procedures

and other security measures. Even so, it is possible for anything to go wrong at some point. The findings of this paper may contribute to greater understanding of how to rebuild people's trust after a data breach, allowing these firms to make an appeal on the necessary data for their activities and realize the increased value and continuation of their business. Furthermore, these organizations could acquire a better knowledge of people' privacy concerns and how these are related to individuals' participation in giving the essential data

VI. THEORY

Trust

According to (Baier 1986) and (Bradley and Campos 2019) patients have historically had a great deal of trust in medical experts. Regarding many societal organizations, trust has long been acknowledged as a crucial element for productive interaction. Regarding the acceptance of increased access to personal information, its significance has been emphasized once again. In the context of healthcare, where patients may present when they are most vulnerable and where they must rely on others for significant and private matters, trust is arguably especially crucial. Trust has been emphasized as a crucial component of successful utilization of electronic health records and other electronically stored health information as it could decrease patients' willingness to accept others' access to and use of their personal data. When patients' needs are addressed and their expectations are upheld, patients are more likely to have faith in the healthcare system (M and Dughan,2001) & (Hawley, 2015)]. Distrust can develop when prior expectations are not satisfied or when there is not what the patient sees as a common understanding. Patients' perceptions of interpersonal interactions and treatment outcomes may be influenced by trust (Damschroder and Neblo, 2010). In situations where trust is high, perceptions and attitudes may influence behavior, which in turn may influence treatment outcomes, which may influence attitudes and perceptions, which may influence behavior, and so on. Low trust may have the opposite effect and create negative feedback loops. High levels of trust may also make it easier for patients to adhere to treatment plans. Individuals who have a high level of trust in healthcare are more likely to seek it out when necessary.

Privacy Concerns

The concept of privacy is a broad definition, which is why this paper fully focuses on the concerns of information privacy. The huge growth of the Healthcare Information System (HIS) has brought forth information privacy concerns (Abdul Rahim and Ismail, 2013). According to articles (Perera and Holbrook 2011) and (Simon and Evans, 2009) patients are becoming increasingly demanding when it comes to maintaining their privacy, particularly when medical professionals are collecting sensitive data. It demonstrates that patients would be more worried about their privacy if they understood the personal significance of their sensitive data. Additionally, it is the duty of healthcare organizations to establish appropriate safeguards for the privacy of sensitive data because these factors may affect the effectiveness of healthcare services through patient satisfaction, adherence, and provider continuity. Patients' privacy concerns will increase if there is a chance of a privacy breach. According to article (Simon and Evans, 2009) patients are extremely anxious about whether sensitive EHR (Electronic Health Records) information will be shared with doctors, other healthcare organizations, or the government. According to article (R and Kaci, 2009), younger clients are more concerned with privacy than older clients are, as they may shield themselves with a variety of privacy-protecting technology. It was suggested that the healthcare organization create a clear privacy framework to identify any potential privacy breach. Guidelines on the actions that should be performed to ensure the privacy of EHR were also strongly advised.

Data breaches

Privacy breaches tend to fall into two broad categories: **internal** and **external** (Hussein and Zarour,2020) In general, a data breach is the unauthorized misuse or disclosure of information. Organizations and people could suffer from data breaches in a variety of ways. Data theft instances not only result in significant financial losses for corporations, but they also damage their reputations.

Internal data breaches are unintended sharing of confidential data with an unauthorized party, or data loss/theft, inauthentic access, and improper disposal of unnecessary but sensitive data. Violations of external data are incidents brought about by an entity or an external source. Examples of external data breaches are a malicious software attack, ransomware attack and any piracy or IT incident.

Data sharing

The term ‘data sharing’ refers to the collection of digital information (e.g., someone browsing on a website) and sharing them between different kinds of parties (Cichy, 2021) With this kind of information sharing, organizations know the digital behavior for people that regularly use the internet. In the case of the Dutch health organization, it is all about the privacy-sensitive information of the

clients. This information should be protected by all costs and should never be disclosed to parties that have no reason to use this kind of information. The data sharing at GGD did not go as expected. Some employees of GGD had access to data of all clients that had been registered at the GGD, this while the employees were not allowed to access the kind of information. This 'error' in data sharing caused the data of millions of Dutch citizens to be leaked.

BRP

BRP is a short term for 'Basisregistratie Personen' which is the database where all the personal data of all Dutch habitants, Dutch emigrants, and some people's data (who have stayed less than 4 months) are also stored (Rijksoverheid, 2022). The Dutch government is doing this kind of registration, to keep everything updated and to have an overview of who and what is in the Netherlands. The security of the BRP is hard to breach, because of the amount of specific people that have access to it. Also, everything in the BRP is monitored, so every step that an employee takes, is noted.

Conceptual model

To identify the impact of data breaches on trust, a conceptual framework is created and represented in figure 1. The framework starts with data sharing, this is the first step in exchanging information between different parties. Every time when data is stored, there is a risk of it being exposed to data breaches. If a data breach occurs, there is a lot of privacy concern regarding the data. This eventually leads to the trust that is impacted from the ones whose data has been compromised.

To calculate the impact on the trust, certain people will be interviewed whose data has been compromised in the Dutch Healthcare. This will help to see what kind of impact it has and how the people are affected by it.

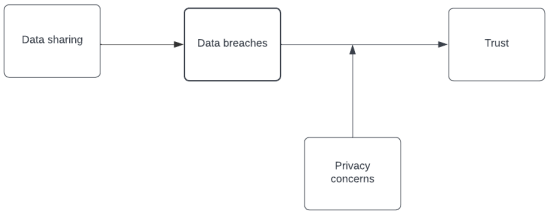

Figure 1: Conceptual model

Hypothesis 0: Data breaches have a 'insignificant' impact on trust

Hypothesis 1: Data breaches have a 'significant' impact on trust

Both hypotheses will be assessed with Cronbach's alpha for reliability and validity. Also, a simple linear regression will be used to analyze the relationship between data sharing and data breaches.

VII. RESULTS

The author's managed to interview 15 people who have been a victim of data breach in the past, Therefore the sample size is 15 (n = 15). The following findings were found following the data's analysis of the interviews using SPSS.

89/**In terms of age categories, 20% of respondents are between the ages of 18 and 30, followed by 67% of respondents between the ages of 31 and 50. 13% of the population is above 50.

About 93% of the respondents had very high trust in health organizations before a data breach happened.

The majority of 67% is very concerned about the security of their personal data as a result of a data breach. While 33% of respondents have some concerns about it.

Moreover 80% of the respondents are not willing to provide particular privacy data in the future when health organizations are in need of it. While 20% of the respondents are not sure about it.

Given that the trust variable is the only multi-item variable, Cronbach's Alpha (Table 1) is used to demonstrate the internal reliability of this variable. For a variable to be trustworthy, it must have a high Cronbach's Alpha.

Variable	Cronbach's Alpha
Privacy concerns	0.149
Trust	0.351
Data sharing	0.661
Data breaches	0.345

Table 1 Cronbach's Alpha

The reliability of a variable must be represented by a high Cronbach's Alpha. If the result is 0.7 or greater, there is a high Cronbach's Alpha, which denotes that it is acceptable. (*NCBI - Diagnostic*, z.d.)

The influence on trust as the dependent variable and the antecedents outlined in the conceptual model is the independent variables. Table 2 shows the result of a simple linear regression analysis result for data sharing on data breaches. The table includes significance levels along with the slope coefficient for B1: Data sharing.

Slope	Correlation coefficient	Significance
B1: Data sharing	0.564	0.029

Table 2 Simple Linear Regression

Finally, table 3 shows the result of a simple linear regression analysis of the relationship between data breaches and trust.

Slope	Correlation coefficient	Significance
B2: Data breaches	-0.777	0.001

Table 3 Simple Linear Regression

The hypothesis that data breaches have a "significant" influence on trust was assessed using this regression analysis. The data of the analysis shows that there is a significant negative impact on trust, thus rejecting the H0 hypothesis.

VIII. DISCUSSION

The fact that not many people were willing to be interviewed is one of the paper's limitations. Finding people who were willing to assist was challenging. By using snowball sampling the authors have gathered a sample size of fifteen persons. Due to this, all variables fell below the acceptable Cronbach's Alpha threshold of 0.7. Beneath this point the Cronbach's Alpha denotes a lack of internal consistency.

Because of the time constraints and the use of the technique snowball sampling, this research had a low sample size and respondents with the same characteristics. As a result of this, generalizability and time constraint also became limitations of this paper.

The fact that the participants are not representative of the population is the fundamental drawback of these non-probability sampling approaches, though. Because of this, this study's generalizability is poor.

Apart from the limitations, the findings of the interviews and data show that there is a considerable negative relationship between the variables data breaches and trust. The data confirms H0 with a correlation coefficient of -0.777. In this context, it indicates that people's trust decreases once they have been a victim of a data breach.

In this study the authors also discovered that most respondents had a high level of trust in health organizations to keep their personal information secure. Few people anticipated that giving their data would result in privacy violations. Nonetheless, when this occurred, many were even more surprised that the assistance provided by these organizations was so limited. The authors have discovered that the assistance provided by these organizations plays a significant role in the issue of trust. According to the interviewees, knowing that you are not alone and that you are being offered assistance or compensation for the data breach helps to decrease the negative impact that a data breach has on trust.

The following can be deducted as advice towards health organizations and its policy makers to reduce the negative impact that data breaches have on trust. Health organizations should offer more help or compensation for data breaches and accompany this compensation with a strategy to decrease the public's anxiety of providing data in the near future. Based on the interviews this can be achieved by communicating the thorough changes that have been made to prevent this event from occurring again. Respondents also indicate that they feel more comfortable with a comprehensive statement of privacy security which they can fall back on, if necessary, rather than a short one.

Figure 2 shows an overview of the results.

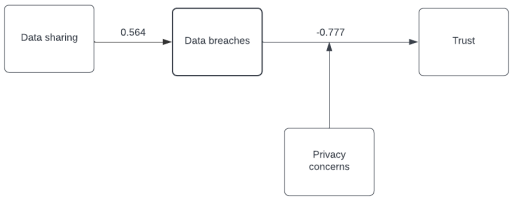

Figure 2: Results conceptual model

IX. CONCLUSION

Data breaches and trust are the two subtopics that this study focuses on because they are the most crucial elements of our research. These elements highlight the importance of having trust in Dutch

Healthcare Organizations when it comes to data sharing and privacy concerns. The conclusion drawn from the findings and discussion is that Dutch health organizations should provide greater support or help during and after data breaches. This guarantees that victims' trust will not be as badly harmed as it may be if health groups had not offered their help or support. Supporting those situations demonstrates the organization's concern for the data of the "victims" whose privacy has been violated and its willingness to assist. Additionally, compensation may be considered (if a data breach occurs). Through interviews with those who have experienced a data breach, **two hypotheses** are investigated in order to assess the connection between trust and data breaches. According to the findings of these interviews, there is a strong negative correlation between data breaches and trust.

Limitations

It became apparent during the research that the sample size was inadequate. Only fifteen persons were interviewed, which is simply insufficient to draw any firm conclusions. The snowball effect strategy was also not the best one to use for our investigation. The ideal scenario would be to obtain a larger sample size, more precise responses, and a clearer understanding of the issue. However, the time frame was too brief when taking into account the time that was available for planning and conducting the interviews. Additionally, not all of the interview questions were insightful. The questionnaire needs to be expanded and better questions that would have an impact on our research should be considered for the following study.

Further research

The prevention of data breaches as well as privacy concerns could be the subject of further research, particularly with an emphasis on government trust. There are numerous models that describe privacy or privacy-related issues. The topic of future research might be the relationship between privacy concerns and trust in the government.

REFERENCES

Abdul Rahim, Fiza, and Zuraini Ismail. "Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review." *Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review*, 2013.

Baier, A. "Trust and Antitrust." *Trust and Antitrust*, 1986.

Bradley, Lott E., and Celeste Campos. "Trust and Privacy: How Patient Trust in Providers is Related to Privacy Behaviors and Attitudes." *Trust and Privacy: How Patient Trust in Providers is Related to Privacy Behaviors and Attitudes*, 2019.

Damschroder, Laura J., and Michael A. Neblo. "Patients, privacy and trust: patients' willingness to allow researchers to access their medical records." *Patients, privacy, and trust: patients' willingness to allow researchers to access their medical records*, 2007.

Hawley, Katherine. "Trust and distrust between patient and doctor." *Trust and distrust between patient and doctor*, 2015.

Hussein, Adil, and Mohammed Zarour. "Healthcare Data Breaches: Insights and Implications." *Healthcare Data Breaches: Insights and Implications*, 2020. *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133*.

M, Hall A., and E. Dughan. "https://pubmed.ncbi.nlm.nih.gov/11789119/." *https://pubmed.ncbi.nlm.nih.gov/11789119/*, 2001.

Perera, Gihan, and Anne Holbrook. "Views on health information sharing and privacy from primary care practices using electronic medical records." *Views on health information sharing and privacy from primary care practices using electronic medical records*, 2011.

R, Elissa, and Liljana Kaci. "Acceptability of a Personally Controlled Health Record in a Community-Based Setting: Implications for Policy and Design." *Acceptability of a Personally Controlled Health Record in a Community-Based Setting: Implications for Policy and Design*, 2009.

Simon, Steven, and Stewart Evans. "Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study." *Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study*, 2009.

Ministerie van Algemene Zaken. (2022, 8 November). *Welke gegevens staan er in de Basisregistratie Personen (BRP)?* Rijksoverheid.nl. https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/gegevens-basisadministratie-personen

NCBI - WWW Error Blocked Diagnostic. (z.d.). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/

Research Methods for Business. (z.d.). Google Books. https://books.google.nl/books?id=ikI6EAAAQBA

APPENDIX A SURVEY QUESTION

Personal questions	
☐	Question 1: What is your gender?
☐	Question 2: What is your age?
General questions	
☐	Question 3: On a scale of 1-5 how much trust did you have in the health organizations before the data breach?
☐	Question 4: On a scale of 1-5 how much did you envision that the sharing of personal data would lead to privacy intrusion?
☐	Question 5: On a scale of 1-5 how much of an impact did the data breach have on your trust in the health organizations?
☐	Question 6: On a scale of 1-5 how concerned are you know about the security of personal data?
☐	Question 7: On a scale of 1-5 to what extent has the government been helpful in helping the victims of the data breaches?
☐	Question 8: On a scale of 1-5 to what extent would the data breach have less impact on your trust if the government would have taken responsibility and actions against the breach?
☐	Question 9: On a scale of 1-5 how willing are you to still provide particular privacy data when health organizations are in need of it?
☐	Question 10: Would your trust increase if the government informed you about changes in the security and privacy statements? Please explain why
☐	Question 11: Do you feel more comfortable with a comprehensive privacy statement or a short privacy statement? Please explain why