Article

Not peer-reviewed version

Patient Privacy Protection Maturity Evaluation Framework

Güney GÜRSEL *, Nükhet BAYER, Ömer TURUNÇ, Abdullah ÇALIŞKAN, İrfan AKKOÇ, Ayhan DEMİRCİ, Melike ÇETİN, Özlem KÖROĞLU

Posted Date: 22 May 2024

doi: 10.20944/preprints202405.1439.v1

Keywords: Evaluation; patient privacy; fuzzy conjoint analysis; similarity

Article

Patient Privacy Protection Maturity Evaluation Framework

Güney GÜRSEL [1,*], Nükhet BAYER [2],Ömer TURUNÇ [3], Abdullah ÇALIŞKAN [4], İrfan AKKOÇ [5], Ayhan DEMİRCİ [6], Melike ÇETİN [7] and Özlem KÖROĞLU [8]

[1] Ph.D., Faculty of Engineering and Architecture, Software Engineering Department, Konya Food and Agriculture University, Konya 42080, Turkey
[2] Ph.D., Department of Health Sciences, Lokman Hekim University; Ankara 06530; nukhet.bayer@lokmanhekim.edu.tr
[3] Ph.D., Antalya Bilim University, Antalya, Turkey; omer.turunc@antalya.edu.tr
[4] Ph.D., Toros University / Healty Management, Mersin, Turkey; abdullah.caliskan@toros.edu.tr
[5] Ph.D., Izmir Tinaztepe University, İzmir, Turkey; dr.irfanakkoc@gmail.com
[6] Ph.D., Toros University / International Trade and Logistics, Mersin, Turkey; ayhan.demirci@toros.edu.tr
[7] Ph.D., Antalya Bilim University, Antalya, Turkey; melike.cetin@antalya.edu.tr
[8] Ph.D., Toros University / Healty Management, Mersin, Turkey; ozlem.koroglu@toros.edu.tr
* Correspondence: guney.gursel@gidatarim.edu.tr; Tel.: 090-532-4753694

Abstract: Background: With the rapid improvement of the healthcare technologies, security and privacy of the most sensitive data, health data is at risk. Protecting patient privacy has many components, even though the data are in electronic format. Although patient privacy is thoroughly discussed in the literature, there is no study presenting all components of patient privacy protection. Methods: In this study, a complete evaluation framework is presented, as an evaluation tool, an inventory is developed, reliability and validity of the inventory is examined. Study is conducted in three phases: Conceptual framework development, inventory development and an evaluation case study. In the evaluation, fuzzy conjoint analysis is employed to handle the subjectivity and ambiguity. As the result of the evaluation, the institution is given a patient privacy protection maturity grade, between 1 and 5, where 1 is the worst and 5 is the best grade. Results: In the case study, XXX's biggest hospital, employing 800 nurses, is evaluated. Half of the nurses, 400, have participated in the study. Literature tells healthcare institutions do not invest enough to protect patient privacy, and the study results support this finding. Institution's maturity grade resulted as level 2, which is bad. Conclusion: The study measures he privacy maturity with many evaluation components. Result of the evaluation explains to the patients and the public if their data is safe or not. With this maturity grade, patients have an idea about which institution to choose, public can conclude the institutions' reliability in terms of patient privacy.

Keywords: Evaluation; patient privacy; fuzzy conjoint analysis; similarity

1. Introduction

Patient Privacy and Security has become very popular especially after the electronic data become a part of health life. Although they are (Privacy and Security) two different things, the term is used as a concept. By security it is meant about how to protect, while by privacy what to protect. Security is related to the storage and transfer of patient data with integrity, validity, and authenticity, privacy is related to the authorized access and disclosure of patient data [1,2].

Patient privacy can be defined as the right of individuals to hide/disclose his health related data from anyone, and control this the data no matter who has it, while disclosing for healthcare, treatment or other reasons [3,4].

Patient health data is the most sensitive data of a person. In case of exposing, it can shame people, cause to feel embarrassed, offended and discouraged, make people lose their job and family. On the other hand, these data can be used for research, education, public health, insurance payments etc. to improve healthcare service.

 doi:10.20944/preprints202405.1439.v1

Health sector's place is in the top three in the yearly reported data security events [5]. Healthcare institutions are direct threat to the patient privacy, because of: [5]

- information system dependence.
- medical device connections.
- multiple software usage.
- multi-user shared devices.

although they help patients by giving healthcare services.

In addition, healthcare staff and other employees' having access to electronically stored or written patient record also present an internal threat. Most of the staff do not take even the simplest precautions because of negligence. User negligence is the major data security breach source [6,7].

Patient privacy can be violated due to the physical problems of health institutions, lack of attention of healthcare professionals, or can be sacrificed to so called protecting patient against risks [8–10].

Patient data is transferred electronically for many purposes, internet of things, homecare solutions, insurance, public health purposes, etc. between systems, devices, organizations. Fast improvement of medical technology brings also new patient data sources such as biometric sensors [11]. Privacy leakage of medical wearable devices is another threat to patient privacy [12,13]. Haris, Haddadi, and Hui [14], examined the privacy leakage risks on mobile computing on mobile and wearable devices. In exchanging patient data electronically with other systems, patient privacy is a major issue that has to be considered in health information exchange (HIE) [15]. Murdoch gave examples about the identification of patients from the anonymized data in which protected health information is removed [16]. The study shows that protected data is also at stake, no matter an institution employs any policy or not.

Despite so many threats and risks on patient privacy, the majority of healthcare institutions do not invest enough to protect patient privacy [16,17].

Protecting privacy and collecting, storing, using health data is a tough balance. So, collection, storage, access, usage, and exposure of these data must be subject to regulations such as law, institutional policy, technical infrastructure etc.

Two big and important regulations on this issue are General Data Protection Regulation (GDPR) and Health Information Portability and Accountability Act (HIPAA).

GDPR imposes obligations onto organizations and people who wants to target or collect data related to people in the EU [18,19]. Although it is not dedicated to health data, it is the toughest privacy and security law in the world.

Health Information Portability and Accountability Act (HIPAA), is a dedicated and detailed patient privacy rule.

Securing and ensuring patient privacy is an ethical obligation of healthcare professionals and institutions, in accordance with the ethical codes and principles [20]. But also, there must be a legal obligation imposed by law just like HIPAA and GPDR. Because violations are done intentionally, unintentionally, accidentally, or negligibly in healthcare institutions by personnel.

The staff should know high penalties are going to be applied for the ones in charge of violation, and the healthcare institution management is the main responsible to apply such controls and fines. To avoid unintentional privacy violations, healthcare staff should be trained. That is the responsibility of the management.

Patient privacy is thoroughly discussed in scientific literature. Blockchain based mechanisms [21,22], AI based studies [23,24], and many other approaches. All these studies have one common objective: ensuring and securing patient privacy while serving the data for better healthcare service.

If there is no defined policy/principle/standard/requisition/prerequisite, it is not possible for healthcare institutions to protect patient privacy. In the literature there are a lot of patient privacy scale/inventory for a wide range of evaluation purposes, but each evaluate only a part, personnel related features, patient related features, system related features, etc. This deficiency prevents us from developing complete mechanisms including all aspects of patient privacy protection, because we can't measure and determine the weak points. We can't manage something that we can't measure, as

 doi:10.20944/preprints202405.1439.v1

the management guru Peter Drucker famously said [25]. In addition, regulations fall behind the rapidly improving technologies they try to govern [16] by being inapplicable or impotent in terms of novel cases and technologies [4].

Because of these problems, the objective of this study is to introduce a complete patient privacy protection maturity evaluation framework, in all aspects, for healthcare institutions. In this framework, in the first step, the arguments to protect patient private data is established and documented. In the next step, an inventory, in which the objective is to measure healthcare institutions' level of patient privacy protection maturity, is developed. The sub aims of the study are listed below.

- Suggestion of the electronically stored and need to be protected minimum and maximum data sets.
- Access mechanisms to these data sets
- Authorization mechanisms of healthcare staff
- Education/Awareness/informing mechanisms of healthcare staff about patient privacy

Because the nurses are the dominating healthcare staff in number and they are directly front facing the patients, the case study is conducted among nurses. In another words, nurses evaluated the institution in which they are working.

2. Materials and Methods

2.1. Ethical Considerations

This study is ethically approved by the XX University Non-Invasive Research Ethical Committee on XXXX with the XX document.

2.2. Study Design

The study is performed in three steps. The arguments to protect patient private data is established first, in another words, conceptual framework is developed, in the second step *patient privacy protection maturity inventory* is developed, then the validity and reliability of the inventory is examined. In the last step, evaluation results of the inventory are examined. Study design is presented in Figure 1.

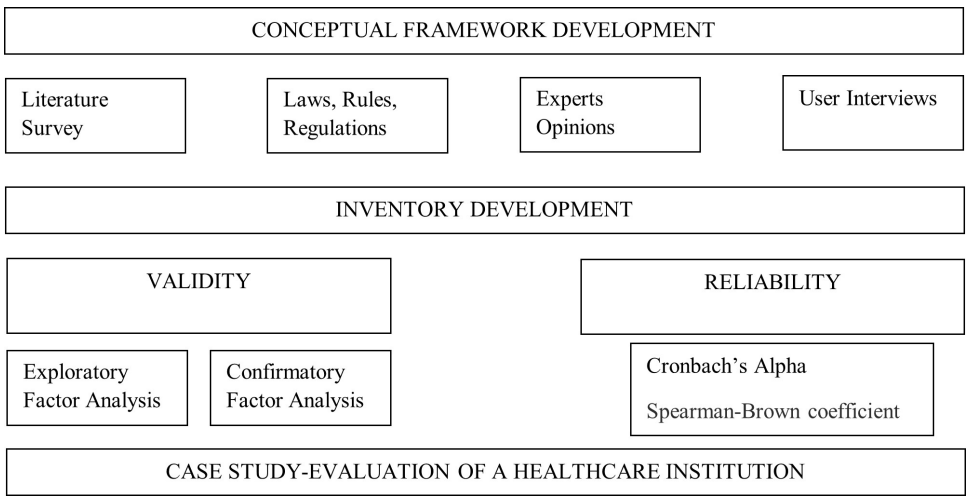

Figure 1. Study Design.

2.3. Conceptual Framework

The dimensions of the Patient privacy protection maturity evaluation framework are:

- Management
- Users
- Patient

 doi:10.20944/preprints202405.1439.v1

- Data
- Healthcare Information System (HCIS)

From the bottom up, the hierarchy of the dimensions is given below in Figure 2. The management is the topmost important part, so it is on the base. Without management support and the things had to be done by management, patient privacy and security cannot be provided. Then the human comes, which is composed of users, patients, and managers namely. Data model is the third part. At the top, the measures, and the mechanisms in HCIS are important.

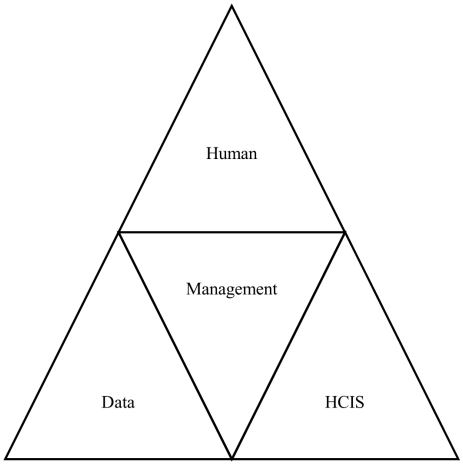

Figure 2. Privacy dimension hierarchy.

The variables of the evaluation framework are given in Figure 3. All the variables and mechanisms are presented below, in detail.

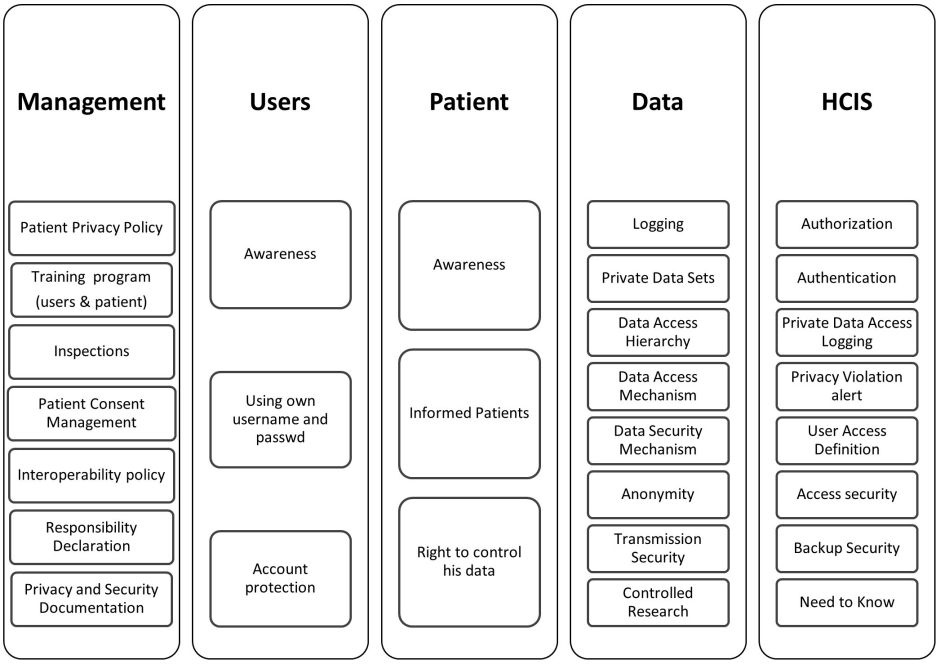

Figure 3. Privacy variables.

Patient Privacy Policy: All healthcare institutions should have a written, approved and declared a public policy about the patient privacy. Patient's rights, institution's and staff's responsibilities together with penalties should be clearly stated in this policy.

Training program (users & patient): All healthcare institutions should train their staff and patients in terms of privacy. In this training, the staff should be trained about the awareness, things to do, things not to do, possible threats, possible outcomes of privacy violations, possible penalties

 doi:10.20944/preprints202405.1439.v1

for both the faulty institution and faulty person. The patients should be trained in terms of awareness, his rights, complaining mechanism, consent, control over his private data.

Inspections: All healthcare institutions should make periodic, planned, or instant inspections about the patient privacy. At the end of every inspection, there should be an effective carrot and stick mechanism. The results of the inspections should be published.

Patient Consent Management: Unfortunately, "Patient consent" is a problem area. Patients are not mature enough to decide on their consent truly. Either they are afraid of not having a good service and give consent although they are not willing to, or they are afraid of something bad (in vain) and do not give consent. They should be informed properly about the procedures and usage of their data, the risks together with their realization rate, etc. to enable the patient to give the right consent and not to give the wrong consent.

Interoperability Policy: In the technology era, the systems are not running alone. There are many other systems and devices interacting with. For a HCIS to be interoperable is a good virtue, but the patient privacy and security should be considered and handled as a challenge. To accomplish this, all healthcare institutions should have a written, approved and declared policy describing the way to interoperate with connecting devices and systems in data exchange in terms of patient privacy.

Responsibility Declaration: All healthcare institutions should have a written, approved and declared responsibility declaration, stating clearly about its responsibilities and penalties in terms of patient privacy and security.

Privacy and Security Documentation: All healthcare institutions should have a privacy and security documentation, to ease human (Users/Patients/Managers) for guidance. It should contain standards, laws and regulations, how-to descriptions.

Awareness: Awareness is a very important issue for human factor of the patient privacy and security. Without knowing an issue exactly what it is and what it is not, one cannot take necessary actions. Human factor of the healthcare institutions should be very well aware of the patient privacy and security.

Using own username and password: The most common violation of patient privacy and security is caused by users' not using their own username and password in healthcare institutions. HCIS users are not sensitive about their usernames and passwords, they give it to other users. As we have stated before, user negligence is the major data security breach source. Considering that all users have different authorization, sharing usernames and passwords means most of the users operate in the HCIS with the authorization that they do not have.

Logging: All the daily operations performed by HCIS users should be stored in HCIS database. This logging history has to be used for possible privacy and security violations, also can be used for retrospective examination in case of complaint or suspicion.

Private Data Sets: All healthcare institutions should have a clearly defined, listed and declared private data set about the patient. This private data set should be subject to special mechanisms both in HCIS and routine use. The proposed private data set derived from HIPAA can be:

- Names.
- All elements of dates (except year).
- Phone numbers.
- Fax numbers.
- E-mail addresses.
- Social security numbers.
- Medical record numbers.
- Health plan numbers.
- Account numbers.
- Certificate/license numbers.
- All means of vehicle numbers.
- All means of device identifiers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) addresses.

 doi:10.20944/preprints202405.1439.v1

- All means of biometric identifiers.
- Any comparable images.
- Any other unique identifying numbers.

Data Access Hierarchy: Having clearly defined the private data set, all the elements of the data set should have an access hierarchy level. That means, all elements should be indicated by means of access security importance level. An example of data access hierarchy is given in Table 1.

Table 1. An example data access hierarchy.

Data	Hierarchy level
Name	7
Phone Number	6
Certificate number	4
Plate Number	4
Social Security Number	7

User Access Definition: By User Access Definition, the healthcare institution defines the level of privacy authorization of the HCIS users. Data Access Hierarchy and User Access Definition help institution manage which user can access which private data set element. An example is given below.

Table 2. An example user access definition.

Data	Hierarchy level
Physician	7
Nurse	5
Technician	2
Lab technician	2
Office Worker	1

When the system combines the user access definition and data access hierarchy, it is seen that a physician can access all the data set given in Table 1 (he has the access definition as 7 which is equal to or greater than all data access hierarchy levels). A nurse can access only to telephone certificate number, plate number. Technician, lab technician and office worker cannot access any private data set element.

Data Security Mechanism: Data security mechanism is a collection of measures to prevent data from unauthorized access and malicious attacks, such as secure protection of hardware, biometric measures, firewalls etc.

Anonymity: Anonymity is an important measure to protect patient privacy. Especially research studies, data exchange, consultations, billing … procedures are very sensitive applications and prone to privacy violations. To protect privacy, anonymity is a good way of solution in such applications.

Transmission Security: In transmission of patient data, the institution should be careful about two stages; the time that the data travels, the time that data is sent and received. There must be mechanisms to ensure the data are not viewed or changed at the time of the travel while on the way.

Controlled Research: Research is very important for development of new technologies/advances/prognosis etc., but there is a danger about abuse and misuse of patient private data. To prevent privacy violation and enable research, there must be a control mechanism, the best solution can be anonymity.

Authorization and Authentication: These issues are very well known and do not need further definition. The only thing that can be made clear may be authorization should be done according to the User Access Definition.

Private Data Access Logging: Any access to private data set should be exclusively logged, separately from the logging defined above. By this special logging, privacy violations can be spotted timely and online.

 doi:10.20944/preprints202405.1439.v1

Privacy Violation Alert: In HICS there can be smart, online alert mechanisms about the potential patient privacy violation, to enable management to prevent a possible case.

Backup Security: While backing up the data in the HCIS database, there should also be mechanisms to prevent privacy violations and protect privacy.

Need to Know: This is a very important principle that can be used to protect security. In access to private data sets, the construction of the user access definition can be referenced according to need-to-know principle. If a user does not need to know an element of the private data set, then the access should not be given.

2.4. Data Collection

Study is conducted, in the biggest hospital in XX country, having 800 nurses employed. Volunteered nurses (400) participated in the study, with a face-to-face interview, and 307 completely answered surveys are analyzed.

2.5. Statistical Analysis

Analysis and measurements are done by means of Statistical Package for the Social Sciences (SPSS) and Analysis of Moment Structures (AMOS).

2.5.1. Content Validity

To measure the content validity of the inventory, experts in the field of nursing and in the field of measurement and evaluation were asked to evaluate each expression in terms of comprehensibility and compatibility. The inventory is arranged and modified according to the feedback of the experts.

2.5.2. Structure Validity

In the beginning, Exploratory Factor Analysis (EFA) is done prior to Confirmatory Factor Analysis. In EFA, Kaiser-Meyer-Olkin (KMO) and Bartlett's tests are used as prerequisite to determine the items' fitness to the Confirmatory Factor Analysis (CFA), in addition communalities are examined. Later, data are analyzed with CFA to confirm validity, reliability, goodness-of-fit testing. For structural validity, fits tests, Comparative Fit Index (CFI), Goodness of Fit Index (GFI), Adjustment Goodness of Fit Index (AGFI), Normed Fit Index (NFI) are used.

In CFA, the most frequently used indicators are chi-square, root- mean-square-error (RMSE), or root-mean-square-error of approximation (RMSEA) [26]. Chi-Square is proved to be sensitive to sample size, it tends to be more significant as the sample size grows, to get rid of that handicap and avoid bias, χ^2/df should be used together with other goodness of fit indexes (AGFI, GFI, CFI, NFI, IFI, and RMSEA) [27]. CFA fit indexes are given in Table 3. [27,28].

Table 3. CFA fit indexes.

	Perfect fit	**Acceptable fit**
AGFI	$0.90 \leq AGFI \leq 1.00$	$0.85 \leq AGFI \leq 0.90$
GFI	$0.95 \leq GFI \leq 1.00$	$0.90 \leq GFI \leq 0.95$
CFI	$0.95 \leq CFI \leq 1.00$	$0.90 \leq CFI \leq 0.95$
NFI	$0.95 \leq NFI \leq 1.00$	$0.90 \leq NFI \leq 0.95$
RMSEA	$0.00 \leq RMSEA \leq 0.05$	$0.05 \leq RMSEA \leq 0.08$
$\chi 2/df$	$2 \leq \chi 2/df \leq 3$	$3 \leq \chi 2/df \leq 5$

2.5.3. Reliability

Reliability of the inventory is examined by Guttman's, Cronbach's Alpha, and Spearman-Brown coefficients.

 doi:10.20944/preprints202405.1439.v1

2.5.4. Evaluation of the Hospital

Data is captured using Patient Privacy Protection Maturity Inventory, developed specifically for this study. In the Inventory, 30 questions exist in which healthcare staff are to express their evaluations/answers using five-point Likert scale, Strongly Agree, Moderately Agree, Not sure, Moderately Disagree, Strongly Disagree. Fuzzy logic methodology, namely Fuzzy Conjoint Analysis (FCA), is used for calculations of the Inventory results. Likert scale context, having ambiguity and multiplicity in meaning, is very suitable for fuzzy logic methodologies. FCA is the statistical and multi criteria evaluation method to determine the value of a product that one appraises and one's preferences related to the criteria employed [29].

Literature has proposed to use fuzzy logic and conjoint analysis together to model the subjective preferences of the evaluators [30].

Likert scales of inventory are converted into fuzzy triangular numbers (fuzzification). In fuzzification, crisp values and linguistic variables of the method is converted into fuzzy sets. In Table 4, the triangular numbers used to fuzzify inventory ratings captured are given.

Table 4. Triangular fuzzy numbers assigned to Likert scales (Linguistic variables).

Data	Hierarchy level
Strongly Agree	0.75, 1, 1
Moderately Agree	0.5, 0.75, 1
Not Sure	0.25 ,0.5, 0.75
Moderately Disagree	0, 0.25, 0.5
Strongly Disagree	0, 0 ,0.25

The membership of each Inventory variable to the defined linguistic variables (our Likert scales), μR(Xj",F" j), is computed with;

$$\mu R(Xj,\mathrm{F}j) = \sum_{i=1}^{n} \left[{}^{wi}/_{\sum wi} \right] . Xi \quad (1)$$

Where;

- wi is the answer given by i-th participant
- ∑Wi is the sum of the answers given to ith inventory item
- wi / ∑Wi is the weight of the i-th participant.
- Xi is the corresponding fuzzy set of the i-th respondents (if the answer is "Moderately disagree" then Xi is (0,0.25,0.5))
- Fj is the jth inventory item.
- n is the total number of answers.

This membership gives us the fuzzy set of each Inventory variable. Now it is time for comparison of these sets with the defined fuzzy sets, and to determine, to the which linguistic variable the given response is closer. Here, the aim is to capture which original linguistic variable is the closest to the final fuzzy set obtained from participants' answers. Similarity is measured by;

$$\mathrm{Sim}(Ri(yj,\mathrm{A}),\mathrm{F}(xj,\mathrm{l}) = \frac{1}{\left[1 + \sqrt{\sum_{j=1}^{n} (\mu Ri\,(yj,A) - \mu F(xj,l))^2}\right]} \quad (2)$$

Where;

- Ri (yj, A) is the fuzzy set determined by 2 (formula 2)
- F (xj, l) is the standard fuzzy sets defined (Table 1)

In the last step of the evaluation, patient privacy maturity score of the evaluated institution is determined. This determination is done according to the similarity values. If the similarity is close to the worst Likert scale, "Strongly Disagree", then the patient privacy maturity score is Maturity level 1, when to the "Moderately Disagree", it is Maturity level 2, when to the "not sure", it is Maturity

 doi:10.20944/preprints202405.1439.v1

level 3, when to the "Moderately agree", it is Maturity level 4, when to the "Strongly Agree", it is Maturity level 5. The higher the maturity score of the healthcare institution, the more mature it is, in terms of patient privacy.

3. Results

400 volunteered nurses have participated in the study,307 of them are included, aged between 22 and 61 with an average of 35,79. 19 participants are female (6.20%) and 288 male (93.80%), 99 married (32.20%) and 208 single (67.80%). 39 participants express their education as high school graduate (12.70%), 36 as BS (11.70%),203 as university (66.10%), 27 as MS (8.80%),2 as Ph.D (0.70%). 29 participants are working in emergency department (9.40%), 12 in operations (3.90%), 31 in surgical departments (10.10%), 137 in internal medicine (44.60%), 41 in administration (13.30%), and 57 in intensive care (18.60).

Before factor analysis, reliability is measured. Cronbach's Alpha, our reliability coefficient, for all 30 variables is measured as 0.973 Spearman-Brown coefficient is 0.949, and Guttman's coefficient is 0.973. Cronbach's Alpha, Spearman-Brown coefficient and Guttman's coefficient according to the dimensions are given in Table 5.

Table 5. Reliability coefficient values.

Dimension	Cronbach's Alpha	Spearman-Brown	Guttman's
Management	0.929	0.870	0.930
User	0.834	0.830	0.834
Patient	0.853	0.768	0.856
Data	0.930	0.906	0.930
Information system	0.925	0.903	0.926

As a pre-requisite to CFA, KMO Measure of Sampling Adequacy (MSA) value, 0.959, is measured to see if the variables fit to factor analysis. The measured value is very close to 1. The Bartlett's Test of sphericity proved to be significant (p=0). These prove research variables are appropriate for a factor analysis [31].

In the EFA, the five dimensions explain a total of 72.175% of the variance among the items in the study. Varimax rotation analysis is evaluated seven times. All communalities were over the required value of 0.500 (between 0.504-.822).

In the CFA, the fit values obtained is given in Table 6.

Table 6. CFA fit indexes obtained in the study together with reference values.

	Perfect fit	Acceptable fit	Study Value
AGFI	$0.90 \leq AGFI \leq 1.00$	$0.85 \leq AGFI \leq 0.90$	0.876
GFI	$0.95 \leq GFI \leq 1.00$	$0.90 \leq GFI \leq 0.95$	0.954
CFI	$0.95 \leq CFI \leq 1.00$	$0.90 \leq CFI \leq 0.95$	0.969
NFI	$0.95 \leq NFI \leq 1.00$	$0.90 \leq NFI \leq 0.95$	0.963
RMSEA	$0.00 \leq RMSEA \leq 0.05$	$0.05 \leq RMSEA \leq 0.08$	0.497
$\chi 2/df$	$2 \leq \chi 2/df \leq 3$	$3 \leq \chi 2/df \leq 5$	2.87

The similarity coefficients and the closest Likert scales of all inventory items are given in Table 7. It is seen that all the items are closer to 'Moderately disagree'. The highest coefficients are marked as bold. In Table 6, the highest value is taken, in another words, the value closest to 1, as explained in methods section. Corresponding Likert scale of the value is the most similar choice we are looking for.

 doi:10.20944/preprints202405.1439.v1

Table 7. Similarity values of the inventory variables.

Variable	Similarity	Strongly Disagree	Moderately Disagree	Not Sure	Moderately Agree	Strongly Agree
M1	Moderately Disagree	0.718218	**0.784835**	0.519829	0.426298	0.384119
M2	Moderately Disagree	0.699176	**0.80075**	0.532724	0.43434	0.390028
M3	Moderately Disagree	0.650733	**0.843053**	0.564349	0.449726	0.398236
M4	Moderately Disagree	0.709998	**0.788945**	0.52799	0.430863	0.386971
M5	Moderately Disagree	0.684141	**0.818907**	0.540279	0.437499	0.39033
M6	Moderately Disagree	0.628925	**0.828878**	0.587218	0.461348	0.403716
M7	Moderately Disagree	0.668136	**0.844412**	0.546092	0.439264	0.390171
M8	Moderately Disagree	0.66005	**0.842132**	0.556088	0.444531	0.393638
M9	Moderately Disagree	0.668635	**0.827864**	0.552673	0.443886	0.393705
U1	Moderately Disagree	0.733799	**0.766653**	0.514777	0.424011	0.382616
U2	Moderately Disagree	0.650898	**0.837291**	0.565584	0.451363	0.39905
U3	Moderately Disagree	0.642923	**0.8332**	0.572724	0.456872	0.403466
U4	Moderately Disagree	0.668369	**0.834325**	0.550549	0.442125	0.393091
P1	Moderately Disagree	0.663697	**0.827674**	0.557226	0.446755	0.396578
P2	Moderately Disagree	0.691294	**0.807406**	0.538052	0.436991	0.391008
P3	Moderately Disagree	0.642528	**0.843339**	0.571963	0.452661	0.398293
P4	Moderately Disagree	0.624436	**0.823395**	0.590312	0.466845	0.409217
P5	Moderately Disagree	0.698044	**0.801263**	0.533885	0.434788	0.388898
D1	Moderately Disagree	0.6586	**0.840305**	0.558345	0.445075	0.393691
D2	Moderately Disagree	0.62853	**0.838854**	0.585223	0.459092	0.402227
D3	Moderately Disagree	0.647867	**0.861636**	0.561251	0.446213	0.393621
D4	Moderately Disagree	0.630309	**0.831065**	0.585698	0.45986	0.403015
D5	Moderately Disagree	0.650272	**0.857155**	0.560497	0.445853	0.393649
D6	Moderately Disagree	0.648802	**0.847849**	0.564973	0.448839	0.396096
HCIS1	Moderately Disagree	0.627952	**0.860448**	0.579846	0.455302	0.39888
HCIS2	Moderately Disagree	0.671541	**0.832493**	0.547898	0.440915	0.39221
HCIS3	Moderately Disagree	0.663280	**0.839029**	0.553546	0.444322	0.394377
HCIS4	Moderately Disagree	0.624389	**0.836324**	0.589115	0.461753	0.404283
HCIS5	Moderately Disagree	0.637784	**0.851736**	0.573845	0.452763	0.397918
HCIS6	Moderately Disagree	0.654471	**0.847441**	0.559831	0.445748	0.394069

The similarity coefficients and the closest Likert scales according to the dimensions are given in Table 8. As in the variables, all close to the Likert scale 'Moderately disagree'.

 doi:10.20944/preprints202405.1439.v1

Table 8. Similarity values of the framework dimensions.

Dimension	Similarity	Strongly Disagree	Moderately Disagree	Not Sure	Moderately Agree	Strongly Agree
Management	Moderately Disagree	0.676446	**0.819975**	0.547471	0.440862	0.392324
User	Moderately Disagree	0.673997	**0.817867**	0.550909	0.443593	0.394556
Patient	Moderately Disagree	0.664	**0.820615**	0.558287	0.447608	0.396799
Data	Moderately Disagree	0.644063	**0.846144**	0.569331	0.450822	0.39705
Information System	Moderately Disagree	0.64657	**0.844579**	0.567347	0.450134	0.396956

4. Discussion

In this study, a complete, patient privacy protection maturity evaluation framework, is introduced. In this framework, healthcare institutions are evaluated in five dimensions under 30 different criteria that have direct impact on patient privacy protection. This evaluation is executed by means of patient privacy maturity inventory, developed specifically for this study, to capture the evaluation data.

According to the validity and reliability analysis, it can be sad that inventory is valid and reliable to measure the privacy protection maturity of a healthcare institution. All reliability coefficients (Guttman's, Cronbach's Alpha and Spearman-Brown) are near to 1, showing very high reliability. EFA shows a high explanation ratio with 72.175%, together with high communality scores. CFA proves almost perfect fit, except AGFI value which has acceptable fit.

It seems as if all participants agreed on the results. Similarity values are very close to 1, changing between 0.76 and 0.86 (in 27 variables >0.8, in 9 variable greater than 0.84), as if almost all users have given the same answer. This shows a complete agreement on the evaluation of the institution.

According to the evaluation results, the institution's patient privacy protection maturity score appears as "Maturity level 2", in all items and dimensions. Meaning; almost, no privacy policy, no training program, no inspections, no documentation, no defined private data sets, no data access mechanisms. This result is compatible with the motivation of the study. If there is no principle/standard/requisition/prerequisite defined, it is not possible for healthcare institutions to protect patient privacy. We have said that securing and ensuring patient privacy is an ethical obligation of healthcare professionals and institutions [21]. In addition, we have said that also an obligation must be imposed by law just like in HIPAA and GPDR. This study results support these assertions. Ethics can be avoided especially when human life, health, or any other good intentioned excuse is on the agenda, or these wonderful excuses can be a shelter to potential violations. As stated before, if legal regulations do not force, healthcare institutions do not invest enough to protect patient privacy [32] and do not spend enough resources [1].

Most privacy violations are found out by the individual (patient/staff/etc) whose privacy is violated, not by an analyst or a smart mechanism [5]. That shows there can be much more violations remain undetected because nobody examines.

This study shows to meet the patient privacy requirements of the evaluation institutions should invest in human and HCIS, by spending time and money, by constructing a body to plan and investigate. This study also show institutions do not take required measures to detect and prevent patient privacy violations in time, before done; most violations of patient privacy are seen when a dedicated investigation is performed, and it is usually too late because violation is already done, and harm is experienced [5].

Not to be late, required measures are supposed to be taken, periodic investigations should be made, and the whole system, all components, should be evaluated.

Managing a healthcare institution with the perfect level of patient privacy protection maturity requires a complete evaluation to prove it is. If it is not at the desired level, we must find out the missing or lacking points. This is possible if and only if you evaluate on the scope of patient privacy.

 doi:10.20944/preprints202405.1439.v1

This inventory may give the institutions to measure where they are in terms of patient privacy protection.

The results of the study prove that the framework and inventory can be used as a measurement for healthcare institutions, it can also be used to construct policies and standards about. This study is only a case study, but it can be applied to different healthcare institutions and verify the model's accuracy with more cases. But with the current obligations and regulations, this study shows the result would not be different.

For further research, the framework can be used to evaluate more healthcare institutions together and analyze the comparative results. The evaluators can be all healthcare staff instead of nurses, and again comparative results between staff can be analyzed. Another version can be using professional evaluators. These evaluators can be trained before the study, then the same team can evaluate different types, sizes, … of healthcare institutions.

5. Conclusions

The biggest significant contribution of the study is its being a complete evaluation framework in terms of patient privacy protection. As it has been stated in the introduction part, although privacy evaluation in healthcare is thoroughly discussed, many evaluation and protection methods are introduced, evaluations are done in only one or a few aspects. In fact, privacy protection is a more complicated issue, and it has many elements which must run together, complete one another, to protect patient privacy. These privacy-protection-complement elements are introduced in this study, as another contribution to the scientific literature.

The framework evaluates the healthcare institution and determines the patient privacy maturity score. The possible scores are Maturity level from 1 to 5, in which higher score is better. By means of this concrete output, the level of maturity of any healthcare institution can be measured, points to improve can be understood, and in the next evaluation, progress in the level of maturity can be seen.

The framework enables us to spot and determine the weak sides and gaps of patient privacy protection of an institution. It can point potential privacy violation issues. This evaluation can be done periodically to examine the maturity improvement on the scope of patent privacy. In addition, we can compare different healthcare institutions in terms of patient privacy protection and rank them from the highest level to the lowest or vice versa. This comparative analysis may be useful especially for the chain healthcare groups, having more healthcare institutions to make inhouse comparisons and build standards.

Author Contributions: Conceptualization, G.G.; methodology, G.G; software, ˙G.G. and N.B. validation, G.G, and N.B.; formal analysis, G.G..; resources, N.B.; writing—original draft preparation, G.G., Ö.K. and Ö.T.; writing—review and editing, G.G.,N.B., Ö.T., A.Ç., İ.A.,A.D.,M.Ç. and Ö.K.; supervision, G.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study is ethically approved by the XX University Non-Invasive Research Ethical Committee on XX with the XX document.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.
Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Sun, W.; Cai, Z. Li; Y., Liu F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. Security and Communication Networks 2018, vol 2018,1-9. https://doi.org/10.1155/2018/5978636.
2. Tertulino, R.; Antunes, N.; Morais, H. Privacy in electronic health records: A systematic mapping study. Journal of Public Health 2024, 32(3), 435-454.
3. Yayla, A.; İlgin, V. E.; Özlü, Z. K. Development of the Perioperative Privacy Scale: A Validity and Reliability Study. Journal of PeriAnesthesia Nursing 2022,37(2), 227-233. https://doi.org/10.1016/j.jopan.2021.06.005.

 doi:10.20944/preprints202405.1439.v1

4. Goodman, K. W. Confidentiality and Privacy. In Hester Micah D., & Schonfeld T.L.(Eds), Guidance for Healthcare Ethics Committees. Cambridge University Press: Cambridge, London. 2022, p. 85-94.
5. Hurst, W.; Boddy, A.; Merabti, M.; Shone, N. Patient privacy violation detection in healthcare critical infrastructures: An investigation using density-based benchmarking. Future Internet 2020, 12(6), 100.
6. Wallace, I. M. Is Patient Confidentiality Compromised With the Electronic Health Record?: A Position Paper. Computers, Informatics, Nursing 2016, 33(2), 58–62. https://doi.org/10.1097/CIN.0000000000000126 PMID:25532832.
7. Jimmy, F. N. U. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) 2024, 2(1), 129-171.
8. Ak, B.; Tanrıkulu, F.; Gündoğdu, H.; Yılmaz, D.; Öner, Ö.; Ziyai, N. Y.; Dikmen, Y. Cultural viewpoints of nursing students on patient privacy: A qualitative study. Journal of religion and health 2021, 60(1), 188-201.
9. Akar, Y.; Özyurt, E.; Erduran, S.; Uğurlu, D.;Aydın, İ. Hasta mahremiyetinin değerlendirilmesi [Evaluation of patient confidentiality]. Sağlık Akademisyenleri Dergisi [health Care Academician Journal] 2021, 6(1), 18–24.
10. Hartigan, L.; Cussen, L.; Meaney, S.; O'Donoghue, K. Patients' perception of privacy and confidentiality in the emergency department of a busy obstetric unit. BMC Health Services Research 2018, 18(978), 1–6.
11. Aslan, A.; Greve, M; Diesterhöft T.; Kolbe, L. Can Our Health Data Stay Private? A Review and Future Directions for IS Research on Privacy-Preserving AI in Proceedings of Healthcare Wirtschaftsinformatik 2022, 8. Retrieved from https://aisel.aisnet.org/wi2022/digital_health/digital_health/8.
12. Kaur, R.; Shahrestani, S.; Ruan, C. Security and Privacy of Wearable Wireless Sensors in Healthcare: A Systematic Review. Computer Networks and Communications 2024, 24-48.
13. Zhang, C.; Shahriar, H.; Riad, A. K. Security and Privacy Analysis of Wearable Health Device. In Proceedings of the IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain (pp. 1767-1772). IEEE. 13-17 July 2020.
14. Haris, M.; Haddadi, H.; Hui, P. Privacy leakage in mobile computing: Tools, methods, and characteristics. Available online: http://arxiv.org/abs/1410.4978. 2020.
15. Shen, N.; Sequeira; L.; Silver, M. P.; Carter-Langford A; Strauss, J.; Wiljer, D. Patient privacy perspectives on health information exchange in a mental health context: Qualitative study. JMIR mental health 2019, 6(11), 1-17. https://doi.org/10.2196/13306.
16. Murdoch, B. Privacy and artificial intelligence: Challenges for protecting health information in a new era. BMC Medical Ethics 2021, 22(1), 1-5.
17. George, A. S.; Baskar, T.; Srikaanth, P. B. Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. Partners Universal International Innovation Journal 2024, 2(1), 51-75.
18. Goldberg, S. G.; Johnson, G. A.; Shriver, S. K. Regulating privacy online: An economic evaluation of the GDPR. American Economic Journal: Economic Policy 2024, 16(1), 325-358.
19. Öztürk, H.; Torun Kılıç, Ç.; Kahriman, İ.; Meral, B.; & Çolak, B. Assessment of nurses' respect for patient privacy by patients and nurses: A comparative study. Journal of Clinical Nursing 2021, 30(7-8), 1079-1090.
20. Wu, H.; Dwivedi, A. D.; Srivastava, G. Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 2021, 17(2s), 1-17.
21. Miao, J.; Wang, Z.; Wu, Z.; Ning, X.; Tiwari, P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems with Applications 2024, 237, 121329.
22. Raj, A.; Prakash, S. Privacy preservation of the internet of medical things using blockchain. Health Services and Outcomes Research Methodology 2024, 24(1), 112-139.
23. Li, F. Research on the Legal Protection of User Data Privacy in the Era of Artificial Intelligence. Science of Law Journal 2024, 3(1), 35-40.
24. Chavali, D.; Baburajan, B.; Gurusamy, A.; Dhiman, V. K.; Katari, S. C. Regulating Artificial Intelligence: Developments And Challenges. Int. J. of Pharm. Sci, 2(3) 2024, 1250-1261.
25. Rychik, J. You can only change what you measure: An argument for more detailed characterization in the Fontan circulation. European Heart Journal 2022,1-3. https://doi.org/10.1093/eurheartj/ehac010.
26. Sebetci, Ö. Enhancing end-user satisfaction through technology compatibility: An assessment on health information system. Health Policy and Technology 2018, 7(3), 265-274.
27. Bastug, M. The structural relationship of reading attitude, reading comprehension and academic achievement. International Journal of Social Sciences and Education 2014, 4(4), 931-946. .
28. Ilhan, M.; Cetin, B. Comparing the analysis results of the structural equation models (SEM) conducted using LISREL and AMOS. Journal of Measurement and Evaluation In Education And Psychology-Epod 2014, 5(2), 26-42.
29. Sofian, S. S.; Rambely, A. S. Measuring perceptions of students toward game and recreational activity using fuzzy conjoint analysis. Indonesian J. Electr. Eng. Comput. Sci 2020, 20(1), 395-404.
30. Turksen, I. B.;Willson, I. A. A fuzzy set preference model for consumer choice. Fuzzy Sets and Systems 1994, 68(3), 253-266.

 doi:10.20944/preprints202405.1439.v1

31. Leech, N.; Barrett, K.; Morgan, G. A. SPSS for intermediate statistics: Use and interpretation. Lawrence Erlbaum Associates Inc: New Jersey, U.S.A. 2013; pp.154-158.
32. Huang, M; Liu, A.; Wang, T.; Huang, C. Green data gathering under delay differentiated services constraint for internet of things. Wireless Communications and Mobile Computing 2018, vol. 2018,1-23. https://doi.org/10.1155/2018/9715428.