2021 IEEE 29th International Requirements Engineering Conference Workshops (REW) | 978-1-6654-1898-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/REW53955.2021.00074

Towards Norm Classification: An Initial Analysis of HIPAA Breaches

Vedarsh Shah
Duke University
vedarsh.shah@duke.edu

Zedong Peng
University of Cincinnati
pengzd@mail.uc.edu

Ganesh Malla
University of Cincinnati, Clermont College
ganesh.malla@uc.edu

Nan Niu
University of Cincinnati
nan.niu@uc.edu

***Abstract*—Regulatory policies, like the US Health Insurance Portability and Accountability Act (HIPAA), impose the social norms mediated by software-intensive systems. Breaches, modeled as norm violations, can help elicit security and privacy requirements to prevent future system failures. This paper reports our initial analysis of 38 HIPAA breaches with the objective of classifying them into the different norm types: commitments, authorizations, or prohibitions. The results show only limited distinguishing power of textual features, and reveal the fundamental interchangeability of commitments and prohibitions.**

***Index Terms*—security and privacy breaches, social norms**

I. Introduction

A *security policy* describes the requirements, regulations, and standards that an organization should meet to protect its assets, and enables technical and social protocols to be implemented accordingly [1]. For example, the US Health Insurance Portability and Accountability Act (HIPAA) is aimed to protect the sensitive personally identifiable information maintained by the healthcare industries from fraud and theft [2].

Due to the wide applicability to diverse individuals and groups, a security policy is often written in natural language. As a result, ambiguity persists regarding how to interpret the legal texts properly. For instance, §170.302(j) of HIPAA states: "Enable a user to electronically compare two or more medication lists." Yet, these medication lists could belong to the same patient or different patients, depending on the comparison's purpose.

One way to reduce ambiguity is through formal representations. To that end, Kafali *et al.* [1] modeled a security policy as a set of *norms*, describing the expectations of users from each other regarding their social interactions [3]. A norm is formalized as: <Subject, Object, Antecedent, Consequent>, and can be classified into three types [1]:

- **C:** A *commitment* means that its subject is committed to its object to bringing about the consequent if the antecedent holds, e.g., <doctors, hospital, media becoming obsolete, disposing of patients' electronic health records (EHRs) from the media> is a **C** norm.
- **A:** An *authorization* means that its subject is authorized by its object to bring about the consequent if the antecedent holds, e.g., <doctors, hospital, emergency, accessing all patients' EHRs> is an **A** norm.
- **P:** A *prohibition* means that its subject is prohibited by its object from bringing about the consequent if the antecedent holds, e.g., <doctors, hospital, ϕ, sharing patients' EHRs with outsiders> is a **P** norm.[1]

A *breach* corresponds to a norm violation [1]. Thousands of HIPAA breaches are recorded by the U.S. Department of Health & Human Services[2], which serve as a valuable source of understanding how the design-time security policy fares in the wild at runtime. Through an ontology matching process between the norms extracted from HIPAA and the norms extracted from 40 representative HIPAA breaches, Kafali *et al.* [1] showed that HIPAA has a general coverage of 65%.

Breaches, thus, are richer than what is prescribed in a policy. They reveal instances where the policy is violated, and can help identify new requirements to enhance security and privacy [4]. In this paper, we focus on the *type* of norms extracted from the breaches, as different types likely give rise to different requirements, e.g., violating an **A** norm may suggest to grant more sufficient accesses, whereas a **P** norm breach could lead to better asset protection mechanisms.

In an attempt to build a practical classifier that will automatically distinguish the norm types, we performed an initial analysis of 38 HIPAA breaches shared by Guo *et al.* [4]. The main contributions of this paper are the term frequency and topic modeling comparisons drawn from various types of breaches, showing rather limited discriminating power of these textual features and provoking some further discussions about norm classification. In what follows, we provide the background information of the HIPAA breach dataset in Section II. We then present our analysis in Section III, discuss some insights in Section IV, and conclude the paper in Section V.

II. Dataset

We took advantage of the HIPAA breach dataset[3] published by Guo and his colleagues [4] where they presented 38 breach reports to the qualified Amazon Mechanical Turk workers for extracting the norms from each breach report. For example, the following breach report:

> "Alleged hackers gained unauthorized access to one or two hard drives on the desktop computers of the covered entity (CE), Dr. Ronald D Garrett-Roe,

[1] The empty antecedent (ϕ) in this example indicates that, *under all circumstances*, doctors are prohibited by their hospital from sharing patients' EHRs with outsiders.

[2] https://www.hhs.gov/hipaa/for-professionals/breach-notification

[3] https://goo.gl/xda2nQ

978-1-6654-1898-0/21/$31.00 ©2021 IEEE
DOI 10.1109/REW53955.2021.00074

TABLE I: Dataset Characteristics

	C	**C&P**	All
# of breaches	30	8	38
average # words per breach	168.80	137.38	162.18
average Flesch reading ease score	21.47	23.43	21.88
average # of norms per breach	1.93	2.25	2.00

> affecting approximately 1,600 patients' protected health information (PHI). The CE reported that the hard drive had been removed, all of the files copied, and the hard drive formatted, which caused all of the computer programs, the operating system, and many patient records to be erased. Dr. Garrett-Roe is no longer a covered entity."

led to a **C** norm: <CE, patients, ϕ, implement sufficient security measures to protect PHI>. Some breach report resulted in multiple **C** norms, such as: <subcontractor, CE and patients, PHI is accessible on the internet, remove server from public internet access> and <business associate (BA), patients, working with subcontractors, obtain proper agreements on data security>. We refer to the breaches leading to only **C** norms as "**C** breaches". In contrast, some breaches in the dataset resulted in the norms of different types, e.g.,

> "On January 5, 2010, BCBSRI was notified that a 16 page report pertaining to Brown University's health plan was impermissibly disclosed to two other BCBSRI agents. The reports contained the PHI of approximately 528 individuals. The PHI involved: first and last names, dates of service, cost of medical care provided, and member identification numbers. Following the breach, BCBSRI recovered the reports, received written assurances that any electronic copies of the reports were deleted, notified affected individuals of the breach, implemented new procedure for all outgoing correspondence, and is in the process of auditing all affected members' claim history to ensure no fraud."

led to the identification of a **C** norm: <CE, patients, ϕ, implement procedure for all outgoing correspondence>, and a **P** norm: <CE, patient, ϕ, disclose PHI improperly>. We refer to these breaches as "**C&P** breaches". We encountered only **C** breaches and **C&P** breaches in the dataset, i.e., no **A** norm was extracted from the 38 breaches, and no breach gave rise to only **P** norms.

Table I presents some characteristics of the **C** breaches, **C&P** breaches, and all 38 breaches of the dataset. **C** breaches are longer. The mean length and median length of **C** breaches are 168.80 and 143 words, whereas the corresponding statistics for **C&P** breaches are 137.38 and 137.5 words. The longer breaches turn out to be a bit more difficult to understand. The readability of the **C** breaches, measured by the average Flesch reading ease score [5], is 21.47. The **C&P** breaches have an average Flesch score of 23.43. Flesch readability index is a score between 0 and 100, with a score of 100 indicating the text is very easy to read and a score of 0 implying the text is very difficult to read. However, both 21.47 and 23.43 fall into the readability band of 10–30, showing that it would typically require a U.S. university graduate to understand all the breaches in the dataset, independent of their types. Due to the length and reading difficulty, as well as the comparable characteristics shown in Table I, we explore in the next section a couple of features to distinguish **C** and **C&P** breaches.

III. Results and Analysis

The two textual features that we investigate in this work are *term frequency* and *topic modeling*. For each feature, we present the relevant literature as our motivations, and then analyze the results from the HIPAA breaches. We discuss the threats to validity in Section III-C.

A. Term Frequency

Term frequency measures a word's number of occurrences in a collection of documents. In our study, we calculate the term frequencies in the **C** breaches and **C&P** breaches, and visualize the results by using word clouds where the more common a word appears in the breach texts, the larger it is displayed.

In the literature of classifying natural language texts, Hakim *et al.* [6] used a term frequency inverse document frequency approach to classify online news articles with a high accuracy of 98.3%. Term frequency inverse document frequency was also employed by Canedo and Mendes [7] for feature selection fed to various machine learning algorithms for classifying software requirements into functional requirements and non-functional requirements, resulting in high F1 scores ranging from 0.87 to 0.91. Interestingly, we drew qualitative insights into the requirements engineering and artificial intelligence literature from the word clouds generated based on term frequency [8], though our focus in this paper is on security and privacy concerns manifested in the breaches.

The word clouds of the **C** and **C&P** breaches are presented in Figures 1 and 2 respectively. As can be seen from these figures, the repeatedly occurring terms of both types of breaches are fairly similar. Both word clouds have mostly the same words being shown, although Figure 1 has many words with similar frequency of occurrences, whereas Figure 2 has a few words with significantly higher frequency than the rest. The most important word with this difference in emphasis is PHI (protected health information)—it has a much higher relative frequency in the **C&P** breaches than in the **C** breaches, indicating that the **C&P** breaches may be dealing more with PHI than the **C** breaches. Despite the above noted differences, our qualitative inspections of the two word clouds suggest that relying on the feature of term frequency would be limited in distinguishing **C** breaches from **C&P** breaches.

B. Topic Modeling

A topic model is a type of statistical model for discovering the abstract "topics", represented by clusters of similar words, which occur in a collection of documents. The assumption is that documents in a collection are generated using a mixture of

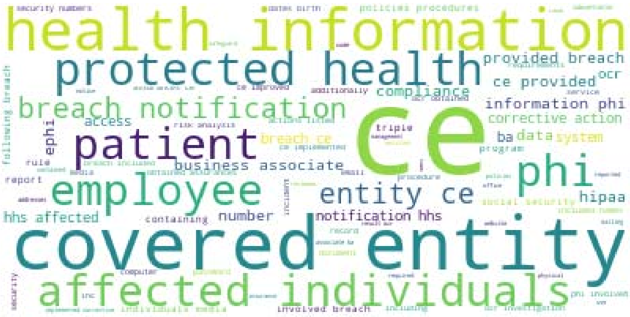

Fig. 1: Word cloud of the **C** breaches.

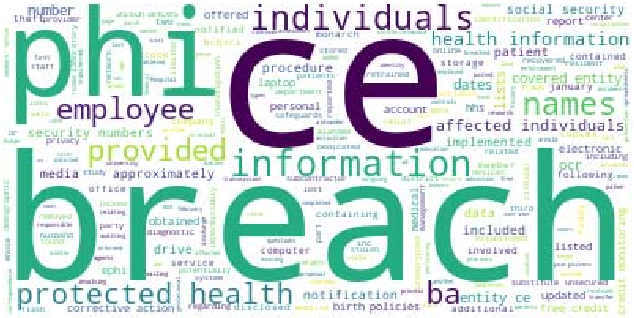

Fig. 2: Word cloud of the **C&P** breaches.

latent topics, where a topic is a dominant theme that describes a coherent concept of the corpus's subject matter.

Latent Dirichlet allocation (LDA) is one of the most commonly used topic models. It can be described as a hierarchical Bayesian model that associates with each document a probability distribution over a number of topics K. In particular, each document is modeled as a finite mixture over K drawn from a Dirichlet distribution. On the other hand, each topic t in the identified latent topics ($t_i \in K$) is modeled as a multidimensional probability distribution over the set of unique words in the corpus. In RE, Mahmoud and Niu [9] applied LDA to recover traceability links, and Bhowmik *et al.* [10] used LDA to perform semantic categorization of software stakeholders' discussions. For example, <'result', 'browse', 'context', 'zoom', 'automatic'> and <'sum', 'start', 'script', 'extension', 'mark'> are two sample topics mined from Firefox's issue tracking system, where each topic is represented by five words.

The LDA topic modeling of both groups of breach texts are summarized in Table II. The table shows the words and their probabilities in each of the five topics of the **C** breaches and also each of the five topics of the **C&P** breaches. C1 is the first topic of **C** breaches, C2 is the second topic of **C** breaches, C&P1 is the first topic of **C&P** breaches, etc. A non-empty cell of Table II means that the word (row) is part of the topic (column), and the numerical value represents the respective probability. An empty cell means the word is not in the topic.

Table II shows that many of the words overlap across topics, both within each breach group (e.g., C1 and C3, as well as C&P2 and C&P5) and across the two groups (cf. Figure 3). Words 1–2 are included in all topics. Words 3–6 are included in all topics except one. Words 7–10 are included in at least four of the topics. Words 11–15 are in at least two topics. Only two topics (C&P1 and C&P4) have more than one word unique to them, resulted mainly from the small collection of eight **C&P** breaches.

To visualize the topic modeling results, we plot five words of two **C**-breach topics and those of two **C&P**-breach topics in Figure 3. Although the probability values vary, the patterns of topic word distribution are similar between C1 and C&P2, as well as between C3 and C&P5. The four topics shown in Figure 3 highlight the covered entity (ce) and its impact on individuals and their protected health information (phi). Thus, our LDA topic modeling analysis does not show any distinct topics within each breach group and also does not show any differences in the topics across breach groups.

TABLE II: Results of LDA Topic Analysis on Both Breach Groups

#	Word	C1	C2	C3	C4	C5	C&P1*	C&P2	C&P3	C&P4†	C&P5
1	breach	0.011	0.019	0.009	0.020	0.013	0.013	0.016	0.029	0.009	0.017
2	individuals	0.009	0.012	0.009	0.016	0.008	0.013	0.019	0.015	0.012	0.020
3	phi	0.013	0.016	0.009	0.017		0.016	0.016	0.013	0.010	0.015
4	ce	0.024	0.035	0.016	0.038	0.018	0.026	0.029	0.030		0.028
5	information	0.010	0.009	0.008	0.020	0.009	0.020	0.022	0.014		0.019
6	health	0.009	0.012	0.008	0.012	0.007	0.011	0.011	0.014		0.012
7	security	0.011	0.009	0.007	0.011	0.006		0.009			0.012
8	ba		0.012	0.007		0.006			0.010		0.014
9	ocr	0.007	0.013	0.008	0.013						
10	affected		0.009					0.010		0.010	0.010
11	protected			0.006	0.012				0.010		
12	covered				0.012	0.009			0.010		
13	entity	0.008				0.009					
14	employee	0.007					0.013				
15	numbers							0.014			0.011
16	patients					0.008					
17	personal							0.009			
18	district								0.010		

*C&P1 also contains the following words (probabilities): lists (0.018), names (0.011), provided (0.011)

†C&P4 also contains the following words (probabilities): reports (0.014), bcbsri (0.014), notified (0.010), medical (0.007), contained (0.007), care (0.007)

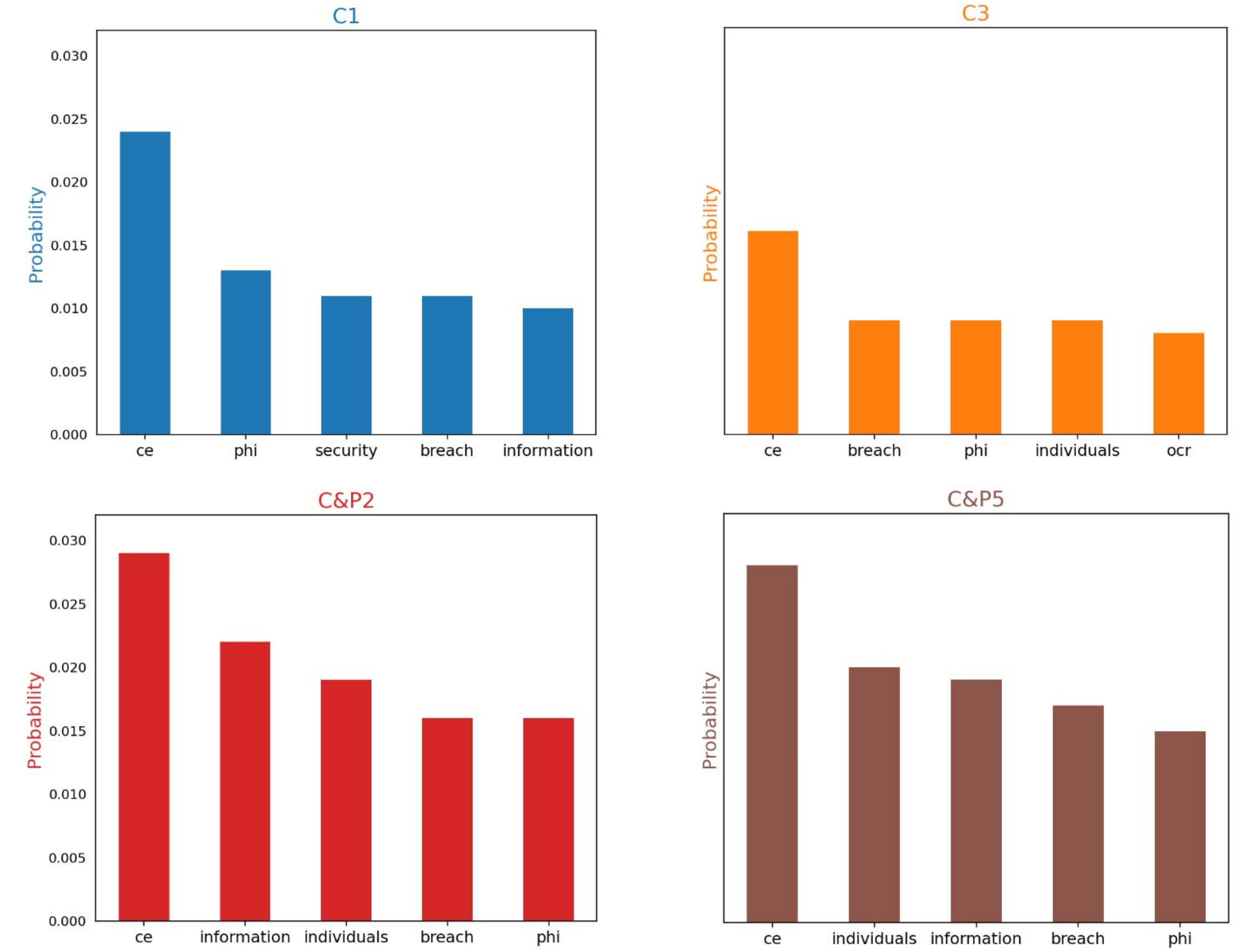

Fig. 3: Words and probabilities of two topics from each breach group.

C. Threats to Validity

Our analysis reported in this section concerns the *type* of breaches, which we adopt the norm classes of **C**, **A**, and **P** [1]. Hence, there is little threat to the construct validity. In addition, the HIPAA breach dataset used in our work was released by Guo *et al.* through their crowdsourcing study [4]. This alleviates researchers' bias of our own team, effectively addressing the threats to internal validity. However, the dataset contained only 38 breaches, which might be too small to obtain significant analysis result.

One threat to our feature selections is the use of term frequency without considering inverse document frequency. Our main rationale is the small number of documents in the dataset. Nevertheless, we performed LDA analysis to complement term frequency by discovering the latent topics from the documents (breaches) in our dataset.

The preliminary results reported here may not generalize to other HIPAA breaches and to breaches of other laws, affecting the external validity of our study. Another threat to generalizability is that the HIPAA breach dataset that we used contains only **C** norms and **C&P** norms. As a result, it is unclear whether the textual features would show distinctive trends for **A**, **P**, **C&A**, **A&P**, or **C&A&P** breaches.

IV. Discussions

Our initial analysis of the HIPAA breaches suggests that neither the length and readability (cf. Table I), nor the textual features of term frequency and topic modeling (cf. Section III) exhibit distinguishing powers for norm classification. While exploring more effective features is part of our future work, we discuss in this section some insights drawn from our analysis.

Along with the similarity among all HIPAA breaches, we discovered that **C** and **P** norm classification is interchangeable. In our dataset, the HIPAA breaches all dealt with the same fundamental problem: an unauthorized individual or group of individuals gaining or potentially gaining access to PHI. The ways in which this occurred varied with each breach:

TABLE III: **P** Norms Rewritten as **C** Norms

Breach ID	Subject	Object	Antecedent (P)	Consequent (P)	Antecedent (C)	Consequent (C)
16	employee	CE	–	disclose PHI to third parties	–	prevent third-parties from accessing PHI
17	employee	CE	portable devices contain PHI	lose portable devices	portable devices contain PHI	protect portable devices from loss
83	CE	patients	–	disclose PHI improperly	–	prevent improper disclosure of PHI
306	employee	patients	–	use personal accounts or devices for work purposes	–	use only approved, accounts and devices for work purposes
495	employee	CE	portable devices contain PHI	lose portable devices	portable devices contain PHI	protect portable devices from loss
510	employee	patients	–	remove PHI from work	–	keep PHI at work
516	subcontractor	CE and patients	–	store data on unsecured servers	–	store data on secured servers
1104	CE	patients	portable devices contain PHI	lose portable devices	portable devices contain PHI	protect portable devices from loss

TABLE IV: **C** Norms Rewritten as **P** Norms

Breach ID	Subject	Object	Antecedent (C)	Consequent (C)	Antecedent (P)	Consequent (P)
2	subcontractor	CE and patients	PHI is accessible on the internet	remove server from public internet access	server contains PHI	make server accessible publicly on the internet
2	BA	patients	working with subcontractors	obtain proper agreements on data security	–	working with subcontractors without adequate data security agreements
6	BA	CE and patients	letters contain PHI	validate contents of letters before mailing	letters contain PHI	mail letters without validating contents
6	CE	–	–	develop policies and procedures about quality control checks on BA	–	have inadequate policies and procedures about quality control checks on BA
11	CE	patients	PHI is stored	implement data loss prevention technology	PHI is stored	leaving data vulnerable to loss/theft/inappropriate access
11	CE	patients	PHI is transported	block transmittal of sensitive information	PHI is transported	allowing easy transmission of sensitive information
11	CE	–	–	improve training of employees	–	have poorly-trained employees
16	CE	–	–	prevent employees from being able to disclose PHI to third parties	–	allow employees to disclose PHI to third-parties

companies mistakenly posting PHI publicly online, robbers stealing an unencrypted computer, hackers hacking into a healthcare provider's server, and letters being mailed to the wrong addresses being just a few examples. This similarity among all HIPAA breaches that we analyzed may have led to the similarities between **C** and **P** norms, instead of a fundamental difference in the breaches themselves.

We therefore made an attempt to rewrite **P** norms to **C** norms while retaining the original meaning, and vice versa. Table III shows the antecedents and consequents of all eight **P** norms in the dataset rewritten to be **C** norms. Table IV shows the antecedents and consequents of eight **C** norms in the dataset rewritten to be **P** norms.

Thus, the two tables show that fundamentally, there is no difference between **C** norms and **P** norms. A norm classified as **C** or **P** can be rewritten to be classified as the other type while retaining its original meaning. Of course, some norms are more straightforward to understand when they are expressed with one classification over the other. However, this shows that the classification of the norms influences the way in which the antecedent and consequent of the norm are worded—it does not influence the meaning of the norm itself.

The lack of a fundamental difference between the two types of norms means that there is also no fundamental difference between **C** breaches and **C&P** breaches. Some of the norms were classified as **P** because they are more straightforward (or natural) to understand when classified as **P** or because the person (e.g., an Amazon Mechanical Turk worker) who wrote the norm thought of it being classified as **P** first, giving secondary or no consideration to the fact that the norm could be classified as **C** as well. This reinforces the earlier findings from term frequency analysis and topic modeling analysis that there are no significant differences in the language used to describe the two types of breaches.

A deeper look at the rewritings presented in Tables III and IV led us to the very definitions of **C** and **P** norms. According to Kafali *et al.* [1], a **C** norm means, "If the antecedent is true, then the subject is committed to bring about the consequent on/for the object." Once we designate the opposite of the consequent to be *anti-consequent*, the above norm can be rewritten as, "If the antecedent is true, then the subject is *prohibited* from bringing about the anti-consequent on/for the object." This gives rise to a **P** norm by definition [1].

Similarly, a prohibition can be expressed as committed to not bringing about the anti-consequent, making it possible to rewrite **P** into the form of **C**. Although changing the consequent to anti-consequent often introduces a double negative, the original meaning is retained and the natural language description (e.g., a breach report) can indeed be classified as **C**, **P**, or **C&P**.

We posit that the interchangeability of the classification of norms from **C** to **P** and vice versa is something that is not specific to norms of HIPAA—it is a property that arises as a consequence of the definition of the norm classifications and thus will arise within any circumstances that these norm classifications are used.

Extending our perspective to **A** norms shows that they are inherently different from **C** and **P** norms. In the sentence form, an **A** norm would read, "If the antecedent is true, then the subject is authorized to bring about the consequent on/for the object." The word "authorized" implies that the subject can bring about the consequent but does not have to do so. This means norms of type **A** have a non-absolute nature, something not observed in **C** or **P**. If the antecedent is true, then a **C** type norm dictates that the subject must bring about the consequent and a **P** type norm dictates that the subject must not bring about the consequent—they are absolute requirements. An **A** type norm, on the other hand, does not dictate that the subject must or must not bring about the consequent. It simply gives permission to the subject and leaves the decision of whether or not to carry out the consequent to the subject—it is a non-absolute requirement.

The implications are twofold. Rewriting an **A** norm into another type, and vice versa, will not be straightforward. Breaches that lead to **A** norms would likely use different wording than **C** or **P** breaches, making the textual features like term frequency and topic modeling potentially useful for accurately classifying this specific type of breaches from the other types.

V. Concluding Remarks

Regulatory text is often abstruse and unclear as to requirements [4]. Breach reports, often legally mandated, describe cases where deployed systems (including software-intensive systems) fail, and suggest actions to prevent, detect, and recover from future breaches [11]. For requirements engineers, breaches not only provide concrete instances where security policies are violated, but also help elicit better ways to evolve the security and privacy aspects of the (software-intensive) systems.

In this paper, we have presented some preliminary results of classifying breaches based on the types of the social norms [3]: commitment, authorization, and prohibition. Our analysis of 38 HIPAA breaches reveals little discriminating power of such textual features as term frequency and topic modeling in separating **C** from **C&P** classes. Our further investigations uncover a fundamental level of interchangeability between **C** and **P** norms, offering a new view on norm classification.

Our future work will expand the dataset of HIPAA breaches and the breaches of other policies and regulations, including the safety requirements [12] and modeling specifications [13]. We are also interested in linking the breaches to policy clauses [14] in order to better interpret the norms and to better implement the security requirements.

Acknowledgment

Funding of this research is provided in part by the U.S. National Science Foundation (grant # EEC-1710826).

References

[1] Ö. Kafali, J. Jones, M. Petruso, L. Williams, and M. P. Singh, "How Good is a Security Policy against Real Breaches? A HIPAA Case Study," in *Proceedings of the 39th International Conference on Software Engineering (ICSE)*, Buenos Aires, Argentina, May 2017, pp. 530–540.

[2] W. Wang, F. Dumont, N. Niu, and G. Horton, "Detecting Software Security Vulnerabilities via Requirements Dependency Analysis," *IEEE Transactions on Software Engineering*, 2020. [Online]. Available: https://doi.org/10.1109/TSE.2020.3030745

[3] M. P. Singh, "Norms as a Basis for Governing Sociotechnical Systems," *ACM Transactions on Intelligent Systems and Technology*, vol. 5, no. 1, pp. 21:1–21:23, December 2013.

[4] H. Guo, Ö. Kafali, A.-L. Jeukeng, L. Williams, and M. P. Singh, "Çorba: Crowdsourcing to Obtain Requirements from Regulations and Breaches," *Empirical Software Engineering*, vol. 25, no. 1, pp. 532–561, January 2020.

[5] R. Flesch, "A New Readability Yardstick," *Journal of Applied Psychology*, vol. 32, no. 3, pp. 221–233, 1948.

[6] A. A. Hakim, A. Erwin, K. I. Eng, M. Galinium, and W. Muliady, "Automated Document Classification for News Article in Bahasa Indonesia based on Term Frequency Inverse Document Frequency (TF-IDF) Approach," in *Proceedings of the 6th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Yogyakarta, Indonesia, October 2014, pp. 1–4.

[7] E. D. Canedo and B. C. Mendes, "Software Requirements Classification Using Machine Learning Algorithms," *Entropy*, vol. 22, no. 9, pp. 1057:1–1057:20, September 2020.

[8] F. Dalpiaz and N. Niu, "Requirements Engineering in the Days of Artificial Intelligence," *IEEE Software*, vol. 37, no. 4, pp. 7–10, July/August 2020.

[9] A. Mahmoud and N. Niu, "On the Role of Semantics in Automated Requirements Tracing," *Requirements Engineering*, vol. 20, no. 3, pp. 281–300, September 2015.

[10] T. Bhowmik, N. Niu, J. Savolainen, and A. Mahmoud, "Leveraging Topic Modeling and Part-of-Speech Tagging to Support Combinational Creativity in Requirements Engineering," *Requirements Engineering*, vol. 20, no. 3, pp. 253–280, September 2015.

[11] M. Riaz, J. Stallings, M. P. Singh, J. Slankas, and L. Williams, "DIGS: A Framework for Discovering Goals for Security Requirements Engineering," in *Proceedings of the 10th International Symposium on Empirical Software Engineering and Measurement (ESEM)*, Ciudad Real, Spain, September 2016, pp. 35:1–35:10.

[12] M. Alenazi, N. Niu, and J. Savolainen, "A Novel Approach to Tracing Safety Requirements and State-Based Design Models," in *Proceedings of the 42nd International Conference on Software Engineering (ICSE)*, Seoul, South Korea, June-July 2020, pp. 848–860.

[13] N. Niu, L. Johnson, and C. Diltz, "Safety Patterns for SysML: What Does OMG Specify?" in *Proceedings of the 19th International Conference on Software and Systems Reuse (ICSR)*, Hammamet, Tunisia, December 2020, pp. 19–34.

[14] W. Wang, A. Gupta, N. Niu, L. D. Xu, J.-R. C. Cheng, and Z. Niu, "Automatically Tracing Dependability Requirements via Term-Based Relevance Feedback," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 342–349, January 2018.