Research Paper
CSCI 530 Computer Security Systems
Katie Foss
StudentID: 2794875038

I have read the Guide to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that is quoted or indented and properly cited to indicated the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such materiel is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to disciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.
Signed: Katie Foss

CONTENTS

Evaluation of RBAC and ABAC to meet Healthcare Industry Access Control Needs

KATIE FOSS

University of Southern California CSCI 530
katiefos@usc.edu

***Abstract*— In 2003, in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the U.S. Department of Health and Human Services (HHS) published the security rule. The security rule aims to protect the availability, integrity, and confidentiality of electronic health information. § 164.312(1)(a) of the HIPAA security rule requires owners of protected health information to implement an access control mechanism to enforce the HIPAA privacy rule [1]. Role-based access control (RBAC) is currently the primary access control mechanism used by the healthcare industry [3], [14]. Attribute-based access control is a newer mechanism and has been suggested as an improvement to RBAC [2], [9]. This paper will evaluate RBAC against the lesser used ABAC to determine why ABAC hasn't replaced RBAC in the healthcare industry. Also presented are suggested improvements to the OCR breach notification database to help improve the adoption of new access control mechanisms, like ABAC in the future.**

I. INTRODUCTION

The HIPAA security rule is comprised of three sections: administrative safeguards, physical safeguards, and technical safeguards. §164.312 is the technical safeguards section, and subsection 1(a) requires healthcare providers who edit, receive, hold, or transmit electronic protected health information to implement access control to abide by the HIPAA privacy rule policy [1].

Early drafts of the security rule required either role-based (RBAC), attribute-based (ABAC), or context-based (CBAC) access control mechanisms (ACM) be used. Ultimately the requirement of a specific mechanism was deemed too strict, and the final security rule focuses on the policy that must be enforced rather than any specific access control mechanism [8].

Of the three original mechanisms listed, RBAC is currently the industry leader [3], [14]. This paper will evaluate RBAC vs. ABAC, as very few publications exist on CBAC in the healthcare space. Section II will introduce the criteria for evaluating RBAC and ABAC to meet health care industry needs. Section III and IV evaluate RBAC and ABAC against the criteria defined in section II. The fifth section discusses the evaluation results and why RBAC is consistently chosen over ABAC, despite meeting all three criteria. Lastly, section VI will propose changes to the OCR breach notification database to help improve access control implementations and foster support for newer access control mechanisms (like ABAC) in the healthcare industry.

TABLE I
SUMMARY OF EVALUATION CRITERIA

Evaluation Criteria	Description
Minimum Necessary	Will the ACM enforce the minimum necessary access to electronic protected health information required for a user to complete their job?
Insider Threat Mitigation	Can the ACM provide finely grained access control to help prevent insider attacks?
Emergency Care Access	Is the ACM capable of handling the "unexpected" user in an emergency care access situation?

II. CRITERIA FOR EVALUATION

Both RBAC and ABAC will be evaluated on the following three criteria: the minimum necessary HIPAA standard, insider threat mitigation, and emergency care access. These criteria were chosen specifically to highlight the similarities and differences between RBAC and ABAC implementations for the healthcare industry. Table 1 provides a summary of the evaluation criteria.

A. HIPAA Privacy Rule Requirement – Minimum Necessary

The HIPAA privacy rule is a separate rule from the HIPAA security rule and provides standards for the "use and disclosure" of protected health information [11]. The security rule specifics an access control mechanism should enforce the policies in the privacy rule. Table 2 shows the privacy rule policies that will be evaluated. These three privacy rule policies combined require health systems who handle protected health information to:

- Identify persons who need access to protected health information (billing, treatment, and health care operations) to carry out their duties [1].
- Classify what protected health information each role requires and under what conditions the access is authorized [1].
- Take "reasonable efforts" to limit access to protected health information to only what is necessary for a user to complete their job [1].

This paper will evaluate RBAC and ABAC to determine if they can enforce the privacy rule to limit access to protected health information to only what is necessary for a user to complete their job [1].

TABLE II
HIPAA PRIVACY RULE POLICY

Title	Section	Summary
Permitted Uses and disclosures	164.506(2-3)	A health provider can use protected health information for treatment, payment, or health care operations without additional authorization [1].
Minimum necessary	164.502(b)(1)	"Reasonable efforts" must be taken to "limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request" [1].
Minimum necessary requirements	164.514(d)(1-3)	"A covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs." [11]

B. Insider Threat Mitigation – Improper Access

Alshehri et al. defined a threat model for evaluating access control mechanisms [6]. They define two insider threats, *unauthorized access*, and *improper access* [6]. Authorization is outside the scope of this paper, so the insider threat mitigation criteria will focus only on improper access. Alsherhi et al. define *improper access* as a user of the system who has valid credentials but is using their credentials improperly [6].[1] To determine if RBAC or ABAC can mitigate the insider threat of improper access, the mechanism must be able to prevent a doctor who is not treating a patient from accessing their record. If the mechanism prevents the access, it will meet this criterion. If the mechanism allows the access, it will not meet the criterion.

Improper access is being evaluated as a separate criterion from the minimum necessary rule because the Office of Civil Rights (OCR) treats the two differently. OCR is responsible for enforcement of the HIPAA security and privacy rule. OCR publishes a database of breaches affecting 500 or more individuals. In OCR's breach database, improper access breaches can be found to satisfy both the security and privacy rules .[2] They are likely treated differently because of the "reasonable efforts" clause in the minimum requirements policy. In many of the entries, OCR lists compensating controls or *after the fact* monitoring as an appropriate technical improvement after improper access is reported [13].

To differentiate the two criteria, the minimum necessary privacy rule criterion will focus on a mechanism's ability to define a role and limit access based on policies applied to the role. The inside threat mitigation criteria will focus on *before the fact* prevention of an insider attack rather than relying on compensating controls to monitor an attack *after the fact*.

[1]In 2008 UCLA staff improperly used their credentials to access Brittney Spears medical records [15]

[2]The OCR database has an entry of a breach submitted on 11/10/2017 affecting 769 individuals. The breach description says "OCR reviewed the CE's policies and as related to this breach and they appear to be in compliance with the Privacy and Security Rules"[13]

C. Emergency Care Access

The last criterion for evaluation is a common access scenario called the "unexpected user". An "unexpected user" is a user who has not been pre-defined in the system [4]. For example, consider a patient Maria arrives by ambulance to a hospital in healthcare system A. Maria normally receives care through health system B. Maria's doctor in system A is not a pre-defined user in system B, therefore has no access to her medical records. HIPAA only requires procedures be in place to share records across health systems [10]. A health system could choose to hire an armed guard to drive a USB from system A to system B, however driving records between health systems doesn't scale. This criterion will focus on whether RBAC or ABAC can accommodate the "unexpected user" to grant (or deny access) automatically.

III. ROLE-BASED ACCESS CONTROL

A. RBAC Overview

Ferraiolo et al. formalized role-based access control in 1992 [5]. RBAC assigned a *subject* (Larry) to a *role* (doctor) and then allows or denies *transactions* (read, write, execute) applied to objects (medical records). Organizations can use the roles and hierarchies which are already well defined to apply access control. Let us consider three organizational roles within a health system, an admin employee in the billing office, a nurse, and a doctor. Each of these roles will require different access constraints. Table 3 depicts an access control matrix (ACM) of these roles and allowable transactions. In the example above, RBAC enforces the permissions laid out in the ACM. A nurse may not order a medical procedure but can read ordered procedures, while an office admin has no need to review medical notes.

B. RBAC Evaluation

While RBAC is industry's primary choice for access control, it satisfies 1 of the 3 evaluation criteria.

1) Minimum Necessary Evaluation: The only criteria RBAC does meet is the minimum necessary criterion. RBAC lends itself well to defining roles and applying privileges based on those roles. All subjects assigned a role have

TABLE III
ACCESS CONTROL MATRIX

Role	Bill	Medical	Procedure Order
Billing Admin	R, W	-	-
Nurse	-	R, W	R
Doctor	-	R, W	R, W

TABLE IV
ACCESS CONTROL MATRIX BY HOSPITAL WARD

Role	Bill	Oncology Medical Record Notes	Oncology Procedure Order
Billing Admin	R, W	-	-
Oncology Nurse	-	R, W	R
Oncology Doctor	-	R, W	R, W
Pediatric Doctor	-	-	-

the same authorization to execute a set of transactions [5]. This means administrators of roles must take special care to design roles to provide the least privilege necessary to complete the role. Table 3 does not provide the least privilege necessary. All doctors in the health system have access to all patient medical records, regardless of whether their role requires the access or not. To meet the minimum necessary requirement using RBAC, many electronic medical record systems grant access by location (hospital floor or clinic), or by department (billing, oncology) [3]. Table 4 shows an example of an access control matrix that could satisfy the minimum requirement.

Consider there are 4 oncology doctors assigned the *Oncology Doctor* role in Table 4. Each doctor has a disjoint set of patients. In this scenario, the four doctors could access medical records of patients not in their care. While the doctors could face serious fines for accessing a record of a patient not in their care, the broader access can be defined as reasonably necessary to carry out their role. In healthcare, speed can make a big difference in care outcomes. If two doctors in the same specialty work together often, it is reasonable to give them the same access.

2) Insider Threat Evaluation: While Table 4 may meet the minimum necessary requirement, it does not mitigate the inside threat of improper access. Recall the scenario of 4 oncology doctors with disjoint sets of patients. If doctor 1 has an ex-husband who is a patient of doctor 2, doctor 1 would be able to read her ex-husband's medical records. RBAC as implemented in Table 3 would not be able to prevent this improper access.

Additionally, RBAC is too coarsely grained to mitigate an insider threat *before the fact*. Coarsely grained access control mechanisms give single users access to large numbers of records. For example, the OCR database lists a breach reported on 6/26/2018 of an inside attack where an employee accessed 4,521 patient records and fraudulently used social security numbers from the records [13]. A more finely grained access control mechanism will be able to mitigate an attack like this better than RBAC.

To try to mitigate an insider threat, administrators of a health system would need to shrink the attack surface. This can be done by creating one role for each health care provider, or one role for each patient. Both scenarios lead to 'role explosion', where more roles are continuously added to create more finely grained access control [4]. Each role created in turn needs to be managed, making such a solution difficult to scale and costly. Because most health systems implement RBAC by department or location, RBAC is too coarsely grained to mitigate the insider threat *before the fact*.

3) Emergency Care Access Evaluation: RBAC requires all subjects be pre-defined by system administrators before an access request can be made [4]. This means RBAC cannot be used to share health records in an emergency care situation and those access requests would need to be handled through another means.

IV. ATTRIBUTE-BASED ACCESS CONTROL

A. ABAC Overview

ABAC builds on the functionality of RBAC and provides three key additional features. ABAC supports multi-factor and dynamic access decisions and does not require a relationship to be pre-defined between subject and object [4].

While RBAC was standardized by NIST in 1992, the closest ABAC has come to standardization is the *Guide to Attribute Based Access Control (ABAC) Definition and Consideration* published by Hu et al. in 2014 [4]. The ABAC model referenced in this paper will come from this guide.

Attribute-based access requests rely on 4 components, subject attributes, object attributes, environment conditions, and policy rules [4]. Attributes are defined as key-value pairs that describe the subject, object, or environment [4]. When a subject makes a request to perform an operation on an object, the subject's attributes are compared to an object's attributes and evaluated against the policy rules and environment conditions to make an access decision. Consider the example in Figure 1, subject A has two attributes: role and *care_for*. In natural language, subject A is a doctor specializing in oncology who cares for patient P. Subject A is attempting to access Object B. Object B is an active medical record of patient P.

Let's consider the policy in Figure 2, according to this policy Subject A would be allowed to access Object B. This policy highlights all three advantages of ABAC. Firstly, the policy is dynamic. The subject can access object B during some parts of the day and not others. Secondly, the policy requires a multi-factor decision. The access decision is based upon three factors, the subject's role, the patients in the subject's care and the time of day. Lastly, the policy does not tie a direct relationship between the object and subject. Because the object and subject are decoupled, a subject does not need to be pre-defined. Only attributes need to be pre-defined. This is particularly evident in who grants access in

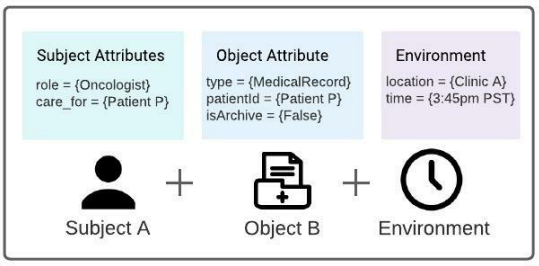

Fig. 1. ABAC Access Request Example

A doctor can read a medical record of a patient in their care between 8am and 8pm.

Fig. 2. ABAC Natural Language Policy Example

ABAC vs. RBAC. In RBAC the owner of the object will define what roles should be given permission to execute certain operations. In ABAC, the owner of the object will define object attributes, but these object attributes are not tied directly to an access decision. It is the policy, which is not owned by the object owner that makes the access decision.

B. ABAC Evaluation

ABAC meets all three of the evaluation criteria.

1) Minimum Necessary Evaluation: Jin et al. formally showed that ABAC can model hierarchical RBAC [7]. To model roles in ABAC, subjects are given a role attribute. Fig 1 and Fig 2 show the policy, subject and object attributes to allow a doctor read access to a patient's medical records under their care. Because ABAC can define roles like RBAC, it too can also satisfy the minimum necessary criteria.

2) Insider Threat Evaluation: Recall, to satisfy the insider threat criteria an access control mechanism must prevent a doctor from accessing a medical record for a patient who is not under his or her care. In contrast to RBAC, ABAC is able to meet the insider threat mitigation criteria. This is because ABAC allows for crafting of finely grained policies. Hu et al. state that *"the policies that can be implemented in an ABAC model are limited only to the degree imposed by the computational language and the richness of the available attributes"* [4]. The policy in Figure 2 is a finely grained policy. To enforce access control of a policy like this, RBAC requires defining a relationship between the subject and object, leading to 'role explosion'. Conversely, ABAC decouples the relationship between subject and object. If a new patient is admitted to the hospital, a doctor caring for the patient would only need a value added to their attribute *care_for*. Nothing needs to be known about the object.

3) Emergency Care Evaluation: In the *Guide to ABAC*, Hu et al. state one of ABAC's strengths is the "ability to accommodate the external or unexpected user" [4]. Recall from the previous example in section II where an emergency room physician from health system A requests access to medical records for a patient in health system B. Pussewalage et al. suggest ABAC could help automatically facilitate emergency care access [9]. Subject attributes are assigned to a subject by attribute authorities. Thus far attribute authorities have all been contained within a single health system, but this is not a requirement of ABAC. Attribute authorities only need to be trusted third parties. For example, the Medical Board of California could be an attribute authority for attribute *physician_license*. Pussewalage et al. discuss one potential solution to providing emergency care access as the following [9]:

- A health system defines an emergency medical record for each patient.
- The emergency record/object should be given the object attribute emergency.
- External physicians who wish to request read access to an emergency record must have a physician license from the attribute authority (licensing board) in their state.
- Policy: Any subject with the attribute *physician_license* can read a record with the object attribute emergency

This solution gives licensed physicians automated access to emergency medical records. However, it is immediately clear this approach could lead to large scale breaches of emergency medical records.

A single adversary could exfiltrate all the emergency records from a hospital system. This could be done by an external or inside attacker. One solution to limit the attack space could be to create additional attribute authorities and define attribute standards to be enforced across these authorities. The following steps would need to be taken:

- A physician requesting read access to an object with the emergency attribute will need to acquire the subject attribute *care_for* of the patient. This means health systems themselves will need to be attribute authorities for the subject attribute *care_for*.
- A system to create and share single unique identifiers per patient needs to be established.
- A standard for defining the *care_for* attribute needs to be defined. This standard would require use of the single unique identifier per patient.
- To prevent adversary attribute authorities from signing a bad *care_for* attribute, an additional attribute authority should be created to sign attribute authorities who meet the *care_for* standards.

This solution is costly, requires multiple organizations to cooperate and would likely take legislative support to accomplish. While ABAC can be used to automate access control for emergency care requests, less costly solutions (like a Health Information Exchange) may be more attractive [3].

V. Evaluation Summary

Tod Ferran is an IT security consultant with over 40 HIPAA risk assessments under his belt. In a private discussion Tod shared he had not seen one healthcare organization implement ABAC, only RBAC [4]. Jon Long is the HIPAA Information Security Officer at Curative, a covid-19 testing

TABLE V
EVALUATION CRITERIA SUMMARY

Policy	RBAC	ABAC
Minimum Necessary	Yes	Yes
Insider Threat Mitigation	No	Yes
Emergency Care Access	No	Yes

laboratory with over 20 million patients. He too in a private conversation shared he has not seen ABAC used.

Table 5 is a summary of the three criteria used to evaluate RBAC and ABAC. ABAC is clearly the winner with 3 yes' to RBAC's 1 yes. If ABAC comes out ahead, why is the healthcare industry rarely, if at all using ABAC to control access to electronic protected health records? I believe the answer is two pronged. Firstly, encoding all real-world scenarios for access control is difficult and potentially prohibitive to providing quality care. Secondly ABAC is still in its infancy compared to RBAC and has multiple open problems.

A. Encoding attributes to protect against an Insider Threat

RBAC has a larger attack space for insider attackers to exploit than ABAC. Why haven't health systems switched over to ABAC to help mitigate this vulnerability? One problem is trying to encode all the possible real world access scenarios [10]. If an ABAC policy limits access to nurses based on predefined shift schedules and patient room mappings, a nurse picking up an extra shift to cover for an employee may lose access to her patients. If ABAC is too restrictive and prohibits a health care worker from carrying out their role, the results could be fatal. The risk of a larger attack space in RBAC needs to be weighed against the risk of reducing the quality of care by potentially slowing down or preventing access to critical documents.

B. Limitation and Complexities of ABAC

There are additional nuances and complexities of ABAC that may also contribute to the hesitancy to switch to ABAC. Servos et al. present a list of ten open problems with ABAC and Hu et al. provide a list of complexities and considerations to make before switching to ABAC [4], [7]. Of these open problems and considerations, 4 are most relevant to the healthcare domain: scalability, cost, auditability, and infancy.

1) Scale: Servos et al. found that "ABAC is still largely unproven in terms of practical scalability" [7]. This is especially true for the healthcare domain. Even if another industry shows it is possible to scale ABAC, the complexity added by HIPAA compliance legislation may hinder the adoption of the mechanism. Secondly, a single policy could require the lookup of many objects, subjects, and environmental attributes. Manging the administrative overhead of many attributes could become burdensome, especially since comprehension of ABAC policies is not nearly as simple as RBAC [7].

2) Cost: Health systems have finite resources. HIPAA requires health systems using electronic health records conduct periodic risk assessments [HIPAA]. These risk assessments help guide organizations on how to best utilize their resources [3]. Unless an organization is repeatedly facing large scale insider attacks, implementing ABAC isn't likely to make the list of security updates. If a system wanted to take advantage of the finer grained and dynamic control offered by ABAC, the cost of implementing ABAC may be prohibitive to making the switch. Not only does an organization have to pay to implement the new mechanism, they also must foot the bill to retro fit all applications to support ABAC [4].

3) Auditability: Once the minimum necessary access is achieved using RBAC, it is simple for administrators to confirm access is properly set up [7]. Administrators can view all subjects that have access to a particular object and all the objects a subject has access to. This is called a *before the fact* audit and is necessary to confirm compliance with the HIPAA security and privacy rule [4]. In ABAC, subjects and objects have no direct link, this makes a *before the fact* audit computationally expensive without proper optimization. Additionally, a policy could contain a large number of attributes, making it difficult for administrators to comprehend and troubleshoot access problems.

4) Infancy: ABAC is not a new access control mechanism and has been mentioned in many publications over the past 20+ years. However, publications pertaining to the applications of ABAC in healthcare are a relatively new. Nweke et al. surveyed 13 papers on applications of ABAC in E-Health Systems, 6 of which pertained to access control of electronic health records. All six of these papers were published within the last 5 years. With very few if any healthcare implementations of ABAC, an industry that deals in life or death will be hesitant to be an early adopter.

VI. FUTURE CONSIDERATIONS

A. Breach Notification Requirements

To help notify the public of data breaches to electronic health records, HIPAA includes a breach notification rule. A breach is defined as *"an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information"* [12]. This rule requires covered entities handling electronic health records to report to the individuals, media, and secretary of HHS when a breach of unsecured data occurs. If the breach affects less than 500 individuals, the covered entity only needs to notify the individuals affected [12].

Table 6 shows four breaches pulled from the database OCR maintains of current and archived breaches affecting 500 persons or more [13]. Breach notification is crucial for shared learning across the healthcare industry to better protect electronic health information. I propose two changes to the HHS database, firstly providing an aggregated summary of breaches and secondly providing more detail on the resolution of breaches. These changes can help covered entities make better choices on where and how to allocate

resources and help with the transition to new and improved access control mechanisms in the future.

1) Aggregated Summary of Breaches: The breach database published and maintained by the Office of Civil Rights (OCR) is a fantastic toolkit to help identify trends in security vulnerabilities across the healthcare industry. Unfortunately, OCR does not publish a summary report of current trends based on reported breaches. It is up to individual organizations to aggregate the data. Both Tod Ferran and Jon Long suggested that an aggregated published report would be helpful in conducting risk assessments [3], [10].

2) Added Details on Resolution: The biggest improvement OCR could make is adding more tabular data. The four examples in Table 6 do not have descriptions but other entries in the OCR database do have descriptions. Some of these descriptions give enough detail to classify what type of vulnerability was exploited, and what resolution was provided. The following is a breach notification description provided by OCR:

"Two former employees of the covered entity (CE), Sentara Healthcare, accessed protected health information (PHI) outside of their normal job duties and used this information to process fraudulent tax returns. The US Attorneyâ€™s office investigated the matter and both individuals received prison sentences. The breach report indicated that the PHI of approximately 3,645 individuals was involved in the breach; however, the CE verified that the final count of affected individuals was 3,891. The CE provided breach notification to HHS, affected individuals, and the media. The CE also offered complimentary credit monitoring and identity theft protection services to all eligible individuals. Following this incident, the CE increased safeguards by installing a new software system to help monitor and detect inappropriate access to its electronic medical records system, updated its security policies and procedures, re-trained employees, and initiated steps to address and mitigate the issues identified in its 2014 risk analysis. OCR obtained assurances that the corrective actions listed above were completed and/or initiated as described" [13]

This description is detailed and identifies that an insider attack occurred and both additional technical and administrative safeguards were implemented. However, these details would be difficult to analyze at scale and aggregate, as they aren't parsed into individual columns. Additionally, it would be helpful to know more about the access control implementation and if it contributed to the breach. For example, was the access control implementation RBAC and were appropriate roles assigned to these individuals to meet the minimum necessary rule? Lastly it would be helpful to know the consequences. This description mentions a prison sentence to the individual attackers, but was the health provider fined? Some of these additional metrics are not yet publicly available and may require legislative support. Other metrics are available, just not easily parsable because they are encoded in a single description column.

VII. CONCLUSIONS

The HIPAA security rule requires an access control mechanism be implemented to protect the privacy of patient data. RBAC is currently the primary choice in industry, but it falls short in mitigating insider attacks and granting emergency access. ABAC has been proposed as an alternative to RBAC by multiple publications [2]. While ABAC technically can meet all three evaluation criteria presented in this paper, ABAC has open problems and complexities which hinder its adoption.

Whether ABAC or another access control mechanism succeeds RBAC, the health care industry is a unique position to learn from past breaches. The breach notification database provides an underutilized tool which can help determine how well access control mechanisms are working and identify best practices for system implementations. Small adjustments to the database could help the industry gain trust in new mechanism implementations and foster shared learning to better protect patient data.

REFERENCES

[1] Office for Civil Rights, "HIPAA Administrative Simplification," U.S. Department of Health and Human Services, Mar 2013. Available: https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

[2] L. O. Nweke, P. Yeng, S. D. Wolthusen, and B. Yang, "Understanding Attribute-based Access Control for Modelling and Analysing Healthcare Professionals' Security Practices," vol. 11, no. 2, 2020, doi: 10.14569/IJACSA.2020.0110286.

[3] T. Ferran, Private Communication, Nov. 2021.

[4] V. C. Hu et al., "Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD; Guide to Attribute Based Access Control (ABAC) Definition and Considerations." Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2019

[5] D. Ferraiolo and R. Kuhn, "Role-Based Access Control," presented at the 15th National Computer Science Conference (NCSC), 1992.

[6] S. Alshehri, S. Mishra and R. K. Raj, "Using Access Control to Mitigate Insider Threats to Healthcare Systems," 2016 IEEE International Conference on Healthcare Informatics (ICHI), 2016, pp. 55-60, doi: 10.1109/ICHI.2016.11.

[7] D. Servos and S. L. Osborn. 2017. Current Research and Open Problems in Attribute-Based Access Control. ACM Comput. Surv. 49, 4, Article 65 (February 2017), 45 pages. DOI:https://doi.org/10.1145/3007204

[8] 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. 2003

[9] H. S. G. Pussewalage and V. A. Oleshchuk, "An attribute based access control scheme for secure sharing of electronic health records," 2016, pp. 1–6, doi: 10.1109/HealthCom.2016.7749516.

[10] J. Long, "Private Communication," 2021.

[11] Office for Civil Rights, "Summary of the HIPAA Privacy Rule," 26-Jul-2013. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[12] Office for Civil Rights, "Breach Notification Rule," 26-Jul-2013. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[13] "Office for Civil Rights Breach Portal," 2021. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[14] M. Jayabalan and T. O'Daniel, "Access control and privilege management in electronic health record: a systematic literature review," vol. 40, no. 12, p. 261, 2016, doi: 10.1007/s10916-016-0589-z. [Online]. Available: https://doi.org/10.1007/s10916-016-0589-z

[15] HIPAA Journal, "UCLA Hospitals Receives $865K HIPAA Fine for Failing to Protect Celebrity Medical Records" [Online]. Available: https://www.hipaajournal.com/ucla-hospitals-receives-865k-hipaa-fine-failing-protect-celebrity-medical-records/

TABLE VI

OCR BREACH DATABASE ENTRIES

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breach Information
Total Urology Care of New York PLLC	NY	Healthcare Provider	23000	9/10/2020	Unauthorized Access/Disclosure	Electronic Medical Record
Texas Family Psychology Associates, P.C.	TX	Healthcare Provider	12000	12/17/2019	Unauthorized Access/Disclosure	Electronic Medical Record
Mercy Health	MO	Healthcare Provider	11187	12/4/2020	Unauthorized Access/Disclosure	Electronic Medical Record
Long Island Jewish Forest Hills Hospital	NY	Healthcare Provider	10333	8/6/2021	Unauthorized Access/Disclosure	Electronic Medical Record