International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

Implementing Role-Based Access Control for Healthcare Data using SharePoint

Venkata Babu Mogili

Independent Researcher, Chicago IL, USA

ABSTRACT: The increased need to have secure and efficient data management in the healthcare has resulted in the use of Role-Based Access Control (RBAC) systems that control access of sensitive information according to the role of the user. The given research is devoted to the implementation of the RBAC system in healthcare data management on the basis of the SharePoint platform that is highly popular in document management and collaboration. The paper details the creation and creation of a powerful access control system, which suits healthcare institutions, considering that it complies with strict privacy laws, including HIPAA. These frameworks involve user authentication, role assigning and data access controls that are incorporated into the SharePoint environment to establish access controls that will be based on defined user roles. The paper goes on to address the issues and best practices when implementing this system including the definition of roles and permissions, dynamic user groups and system scalability. The case study is offered to illustrate how the framework has been effective in a healthcare environment, and how it enhances data safety, efficiency, and compliance with regulations. The study provides the audience with the prospects of SharePoint as an elastic and scalable software to handle healthcare information and provide a secure access control system. The next step in work will be the optimization of the framework to cover the new challenges of healthcare data management.

KEYWORDS: Role-Based Access Control, Healthcare Data, SharePoint, Data Security, Access Control Framework, HIPAA Compliance, Healthcare IT.

I. INTRODUCTION

The healthcare sector is among the most data sensitive sectors in the world, and mass amounts of personal health information (PHI) are being created, distributed, and stored on a daily basis. As digital platforms are becoming more widespread in controlling healthcare data, it is more essential to make sure that the information provided is safe and can be accessed by authorized personnel only. Role-Based Access Control (RBAC) has been one of the security models that has acquired popularity among other models because it is effective in controlling the access of users based on the roles they undertake within an organization. In this study, the authors will examine how RBAC can be applied to healthcare data with the help of SharePoint, a unified platform that is popular in the sphere of managing documents and collaborating in the organizations across the globe. The aim is to develop a framework that will provide the necessary level of data security and at the same time ensure ease of use and compliance with regulatory policies in the healthcare industry [1].

Cyber criminals usually target healthcare data because it is sensitive. The personal health information could be disclosed or lost and that could be disastrous, as the results could be identity theft, fraud and even damages to individuals. Moreover, health institutions are undergoing more scrutineous and regulatory demands to allow them to safeguard confidential patient information. The United States is one example where the Health insurance Portability and Accountability Act (HIPAA) helps ensure tough rules to follow in the reception and protection of PHI. Data protection is not a recent issue in healthcare providers as there are similar regulations in other countries, like the General Data Protection Regulation (GDPR) in Europe [2] [3].

To address these threats, health care organizations have to adopt effective data protection policies that limit sharing of sensitive data except to the necessary staff who will be able to access the necessary data to fulfill their responsibilities. This has seen the implementation of security models such as RBAC in which access is provided to users depending on their positions in the organization and not on ad-hoc fashion.

RBAC is an access control model and it is used to assign permissions to users regarding their role in an organization. A role is a set of duties and rights demanded to accomplish some tasks. Access to each role is restricted to certain access privileges and roles are assigned to users depending on their duties. An example is that a medical practitioner can be in

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

various positions where he/she can be a doctor, nurse, administration, and medical records and have varying degrees of access to patient information [4].

The benefits of RBAC are many. It offers an organized, sensible, and controllable way of managing access control in a complicated system such as healthcare organisations. RBAC is an easy way of managing users by minimizing the number of permissions granted to specific users. It also improves adherence of privacy policies, since it will enable administrators to implement data access policies at the role level. Additionally, RBAC enables the concept of least privilege so that a user can only access the minimum authorization to execute the required duties to limit the chances of data leaks.

RBAC can be used in the healthcare sector to provide a fine-grained access control to patient data, which may need to be viewed, edited, or deleted by the user, and is necessary to preserve the privacy of patients and fulfill the requirements of various regulations such as HIPAA. To illustrate, a physician might have a full medical history of a client whereas a nurse might have a partial access to a medical history of a patient as it pertains to his or her care.
SharePoint is a popular collaboration tool which is created by Microsoft and which is a tool that combines document management, collaboration and storage. SharePoint is a tool that is necessitated by the need to manage document, workflow, and data in organizations of all sizes and across all industries over the years. As a healthcare organization, SharePoint can be utilized as a centralized data storage and management facility of the healthcare information, such as patient records, medical images, and treatment plans [5].

Flexibility is one of the major aspects of SharePoint. It enables the organizations to develop their own workflows, set access control, and develop content management policies. The above characteristics make it a perfect platform upon which RBAC can be applied in a healthcare facility as it allows organizations to effectively control access by users, as well as to secure sensitive data. SharePoint has an inherent ability to create user roles and permissions, which means that healthcare organizations can easily execute RBAC without creating solutions.

Besides, SharePoint is fully interoperable with other Microsoft Office products, including Word, Excel, and Outlook which are widely used in the healthcare facilities. This integration ensures the ease with which the data sharing, communication, and collaboration between the professionals in the health sector. Nevertheless, the security features that SharePoint has are well-established, yet they should be thoroughly configured to address the strict provisions of healthcare data security.

Although Sharepoint offers the required means to set up RBAC, establishing an efficient access control system of healthcare information is sophisticated. Healthcare organizations should not simply make sure that the access is limited in accordance to the roles but also make sure that they do not violate several healthcare-related regulations. This includes the creation of a structure that takes into account the unique requirements of healthcare professionals, like the ability to give the doctors full access to data on patients but not to administrative personnel.

Compliance is not the only aspect of an effective RBAC system that should be considered. Medical workers frequently have to complete their tasks fast and correctly, and any obstacles on the way to the required information may impact patient care negatively. Hence, this necessitates the development of an RBAC that is secure and easy to use and reduces the time that the healthcare workers will take to access the data they need [6].

The study will address these issues through the design and implementation of an RBAC framework specific to healthcare data management in Sharepoint. The framework will be based on compliance with the healthcare data protection regulations, better data protection, and the user experience of healthcare professionals.

The main aim of the research is to come up with an RBAC model of managing healthcare information through SharePoint. The framework will be structured in such a way that it is aimed at:

1. **Enhance data security**: Through the adoption of RBAC, the research will limit access to user-related healthcare data (depending on their roles) and reduce the chances of information being accessed improperly.
2. **Ensure regulatory compliance**: The framework will be structured to meet applicable healthcare laws including the HIPAA and GDPR so that the data access policy is legal.
3. **Improve operational efficiency**: The framework will enable healthcare organizations to support their data management processes in order to reduce administrative overhead and maximize productivity by simplifying access management with the help of role assignments.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

4. **Provide a scalable solution**: The framework will be modeled to meet the increasing demands of healthcare organizations to make sure it can be expanded as the organization increases in size and introduces new positions or departments.

The area of this study is the design, implementation and testing of the RBAC framework of the SharePoint platform. To illustrate that the framework remains effective in a real-world situation, a case study of a healthcare organization will be provided. Some of the pitfalls that are likely to arise when applying RBAC in health facilities like the definition of roles and permissions, and management of dynamic groups of users will also be discussed in the study.

II. RELATED WORK

Role-Based Access Control (RBAC) systems applied to healthcare data management have been getting a lot of attention in the recent years because of a growing need to have effective security mechanisms through which the confidentiality of patient data is assured and regulatory assurances met. The use of RBAC in healthcare systems has been the focus of many studies which have proved that it is effective in controlling access to confidential health information depending on the roles of users in an organization.

The development of RBAC frameworks in different industries and the healthcare industry in particular is one of the areas of related work. These structures have a tendency to underline the significance of establishing explicit user roles, as well as, assigning user roles the relevant authority. As an example, in healthcare facilities, the typical users like doctors, nurses, administrative personnel, or medical researchers need access to varying degrees of medical data like patient records, clinical notes, or diagnostic information. Such role-based access controls can be narrowed to allow only qualified staff to have access to certain kinds of data, which reduces the chances of data breach to a minimum. Moreover, there are numerous frameworks that focus on the principle of least privilege, which presupposes that users have access to only the minimum amount of access that they need to perform their tasks to minimize the risk of either accidental or deliberate access to sensitive information.

The use of RBAC in the platforms and technologies of existing healthcare is another area of concern. A number of studies have been dedicated to the combination of RBAC and Electronic Health Record (EHR) systems, hospital management software, and other healthcare IT infrastructure. In many of such integrations, access control mechanisms in such systems are usually customized to meet the needs and roles of healthcare professionals. Combining RBAC with these platforms allows control over user privileges comfortably and makes sure that access to the data is controlled in different applications and departments of healthcare organizations. In addition, the discussion of the integration of RBAC with identity and access management systems has also been discussed since there is an opportunity to have more centralized control over user authentication and access rights [7].

The other important aspect in the design and implementation of RBAC systems in healthcare is healthcare regulations like the HIPAA and GDPR. These laws take the strict control over sharing and protection of information of patients, which is ultimately reflected in the design of access control systems. The importance of RBAC in the regulatory compliance with these regulations is not a secret and numerous studies in this regard are conducted to emphasize the significance of developing access control policies that comply with legal and ethical provisions. This involves making sure that sensitive data is not made available to people who do not need to know such information according to their duties at the workplace. In addition, there have been efforts of development of auditing system in RBAC system to trace and log access to sensitive information, thereby allowing organizations to have a comprehensive history of all user activities and to adhere to the regulatory needs [8].

About the issues of implementation, a number of studies have indicated the problems that organizations encounter in defining user roles and dealing with dynamic alterations in the staff roles. Role definitions are usually not up to date as the healthcare organizations usually experience a high turnover rate and constantly changing job functions. Other studies have suggested remedies like using machine learning algorithms to automatically allocate roles and permissions on the basis of user conduct, and other has concentrated on designing a more adaptable RBAC design that can readily adapt to changes in the user roles.

Also, an issue of concern has been the user experience of RBAC systems in a healthcare environment. Medical workers usually face time pressure and have to get immediate access to information. Excessively complex or restrictive access control may impede the workflow and slow decision-making, which may affect patient care. Consequently, there have been studies on the issue of optimizing security and user-friendliness where some systems have been suggested to

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

enable healthcare workers to retrieve the required data in the shortest amount of time possible without compromising on security measures. These involve the adoption of single sign-on (SSO), context aware access policy, and role specific dashboards that can facilitate easy access without jeopardizing security.

Lastly, another area of concern in regards to RBAC systems has been the scalability of the system. The number of users can be hundreds and even thousands of users within healthcare organizations, especially large hospitals or healthcare networks, who need varying degrees of access to huge amounts of data. Leveraging the need to develop RBAC systems that can scale effectively and handle the complexity of the user roles and permissions has drawn the attention of numerous studies. It has been proposed that hierarchical RBAC models can be used with roles organized in a hierarchy and it can be more convenient to manage the permissions within large organizations. The use of cloud-based solutions has also been discussed by others which provide the scalability and flexibility required to support access control of a large and distributed healthcare environment.

In short, as much effort has been made to deploy RBAC systems in the health care world it is not possible to have an appropriate user role assignment, carrying out required regulatory compliance, efficient user experience, and scalability. With the healthcare industry continually changing, the creation of flexible, efficient, and secure models of RBAC implementation will be essential in protecting patient information and in the proper operation of healthcare organizations.

III. FRAMEWORK FOR IMPLEMENTING ROLE-BASED ACCESS CONTROL (RBAC) IN HEALTHCARE DATA MANAGEMENT USING SHAREPOINT

Access control to patient sensitive information is one of the issues in healthcare organizations because it is a growing trend in the number of digital records, and privacy and security demand high standards. Role-Based Access Control (RBAC) is one of the effective methods that can be used in the management of access; this also controls data accessibility depending on the role of the people in an organization. This part outlines a detailed model of RBAC application in SharePoint that is a popular collaboration and document management system to help manage healthcare data in a secure and efficient manner. The suggested framework will be able to improve the security of the data, guarantee the adherence to the healthcare regulations (e.g., HIPAA, GDPR), and make the user experience of healthcare professionals more streamlined due to the ability to access the data in the right way. The framework below is designed in a way that it tackles the important aspects of role definition, user authentication, permission management, data access controls, and regulatory compliance. The framework also has the provisions on scalability, auditing and monitoring to make sure that the access control system is strong and flexible as the healthcare organization expands.

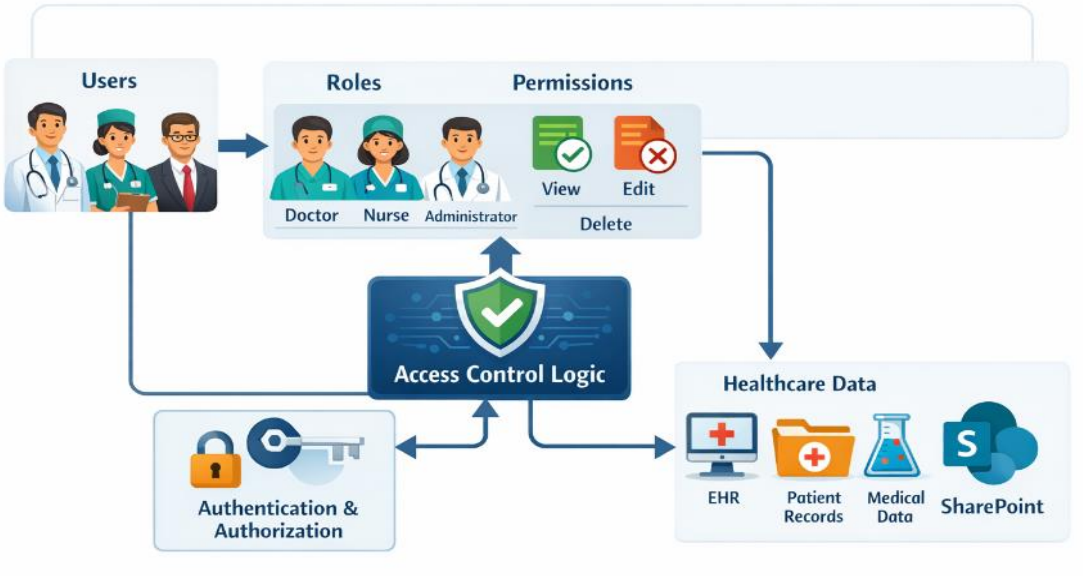

Figure 1: Role-Based Access Control Architecture for Healthcare Data Management

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

1. Role Definition and Granularity

Any RBAC system is based on the definition of clear roles and specification of particular access permissions depending on the roles. Within a healthcare environment, roles are generally set on the responsibilities and duties of a healthcare professional, administrative staff and other employees. To illustrate, some typical categories of users are doctors, nurses, medical technicians, administrative personnel and healthcare managers, and each of them needs access to patient information, medical records, or organizational papers on varying levels.

The initial phase in the implementation of RBAC in SharePoint is the definition of the different roles in the healthcare organization. This must be done in partnership with other important stakeholders, including the administrators of the health care organization, information technology personnel, and clinical representatives to make sure that the functions are based on the needs and also on the workflow of the organization. A normal breakdown of functions within a healthcare organization is as follows:

- **Doctors**: Generally require the entire medical history, diagnosis, treatment plan, laboratory results and medical history.
- **Nurses**: Require information on the treatment and care plans of a patient, but not full medical history or confidential information such as diagnostic reports.
- **Medical Technicians**: Require information on the treatment and care plans of a patient, but not full medical history or confidential information such as diagnostic reports.
- **Administrative Staff**: Typically need to get non-medical information, including patient appointments, billing data, and simple contact points.
- **Healthcare Managers**: May should have access to aggregated data to use in reporting, managing patient care and performance tracking but should not access detailed medical records unless it is necessitated by their position.

These roles are to be given designated permission to reach certain sets of data in SharePoint. An example of this is that a doctor can have access to view, edit, and share medical records whereas the administrative employees can only have access to view and manage patient appointment schedules. SharePoint has user group management tools that allow such permissions with various levels of access which include, Read, Contribute, and Full Control.

Along with role-based permissions, the framework must provide the ability to create role hierarchies, whereby senior roles (e.g., healthcare managers) have more access privileges than junior roles (e.g., nurses). Hierarchical RBAC model assists in simplifying access control, especially in large hospitals.

2. User Authentication and Identity Management

The process of ensuring that users who are seeking access to the healthcare data stored in SharePoint are true to their identities is known as user authentication. To ensure a secure implementation of RBAC, it is important that the authentication systems should be sound and not allow unauthorized access of sensitive healthcare data.

The system utilizes the features inherent in the SharePoint which improves the active directory (AD) to control the user identities. Through active Directory, one is able to have centralized management of user accounts, group membership and access policy. The roles are associated with user accounts depending on the job functions and ensure that the access is provided at the right level, depending on the role of the user in the healthcare organization. When a user tries to log into the SharePoint, the system matches the credentials of the user with the directory to confirm their identity and then it provides them with access.

Besides conventional authentication systems (e.g., the username and a password), the framework needs to be compatible with multi-factor authentication (MFA), which will provide an additional security system. MFA will compel the user to enter two or more authentication factors, e.g., a password and a code delivered to their mobile phone and will therefore make it much more difficult to access the system by an unauthorized user.
In the context of healthcare organizations that are present in different locations, single sign-on (SSO) services are to be implemented to enable healthcare professionals to authenticate themselves only once and receive access to diverse systems, such as SharePoint, without reentering their credentials. This enhances convenience to the user and provides interoperability in authentication.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

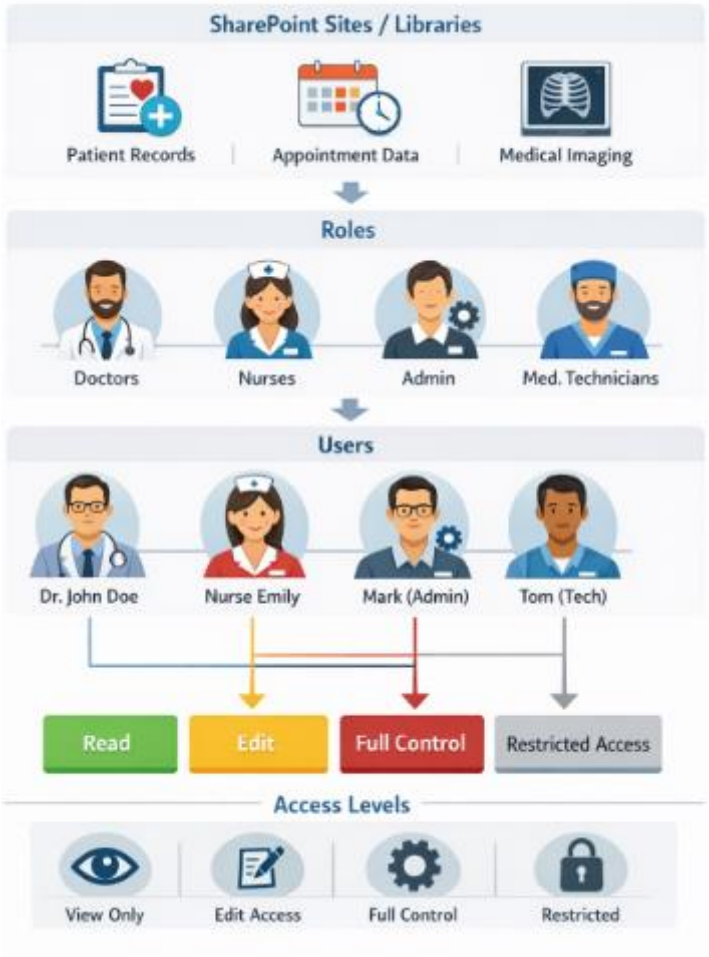

Figure 2: SharePoint Permission Hierarchy and Role Mapping

3. Permission Management and Data Access Controls

After defining roles and authenticating users, the next thing is to control permissions and implement granular access controls to control access and sharing of healthcare data. SharePoint offers variety of access control features that can be tailored depending on the roles that are identified in the RBAC framework.

All the permissions can be granted at various levels within share point and these are: site, library, document and list. The administrators can control the access to various types of data without much effort by sorting healthcare data into clear SharePoint sites and libraries. An example is to have patient records stored in a separate site collection with limited access and general organizational data such as the schedule of patient appointments that are kept in a different site with a wider access.

The following aspects of permission management are also inside the framework:

- **Role-based Permissions**All the roles have permissions which allow a user to do what he/she can. These activities involve reading, modifying and deleting or sharing documents, administration of lists and libraries.
- **Access Control Lists (ACLs)**: SharePoint also allows defining the users or groups of users who should be allowed to access a particular document or resource and that can be achieved using ACLs. The RBAC model makes sure that each document or data set is related to a suitable ACL in regard to the role of the user.
- **Delegated Access**: There are instances where there might be temporary or delegated access. As an illustration, a physician might be required to give another colleague temporary access to his or her medical records. This feature is facilitated by the framework through the creation of temporary roles or permissions by the administrators.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

- **Context-Aware Permissions**: Its framework can also feature context-sensitive permissions that can vary the access depending upon certain factors, including time of day, location of user, or type of device. This can be used to secure sensitive data by making sure that only secure conditions are used in accessing the sensitive data.

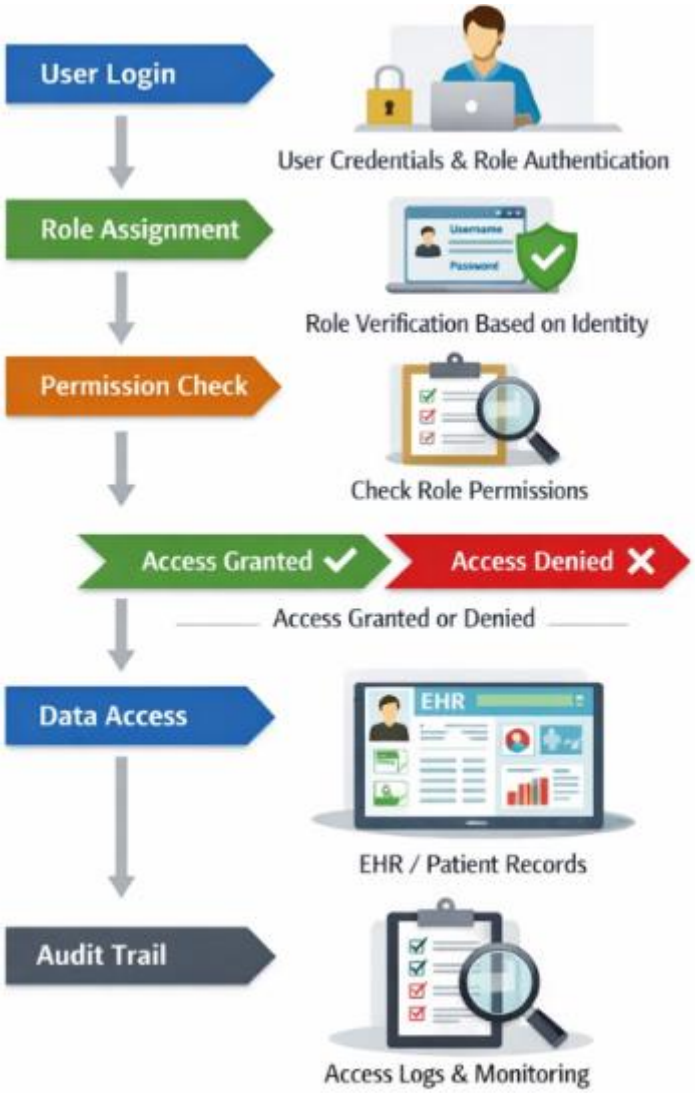

Figure 3: Data Access Workflow in RBAC for Healthcare

4. Compliance with Regulatory Standards

The primary reasons behind introducing RBAC to healthcare are the need to guarantee the adherence to privacy laws such as HIPAA in the United States or GDPR in Europe. These laws force healthcare institutions to take strict actions in order to safeguard the patient information and make sure that sensitive information is accessed by authorized personnel.

This RBAC architecture in SharePoint is set to be compliant with these regulations, through the policy of access control to the information, which restricts the access to the data to the authorized users. Besides restricting access by roles, the framework has other provisions of auditing and recording access to sensitive data which is necessary as per regulatory standards to monitor and report to the same.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

Key compliance features of the framework include:

- **Auditing and Monitoring**: SharePoint also has powerful audit features, which are able to monitor the actions of users, such as accessing documents, making changes and deleting of the documents. These auditing features must be set up by the RBAC framework to track access to sensitive healthcare information so that any unauthorized access to the same is recorded and noted to be reviewed.
- **Data Retention Policies**: The architecture must facilitate the adoption of data retention policies that guarantee the retention of the patient records as long as it is necessary and deletion of these records at the end of the retention period in a secure manner. These policies can be implemented by use of the retention settings in SharePoint.
- **Access Reviews and Certifications**: As a way of ensuring compliance, access reviews should be done regularly to ensure that sensitive data is only accessed by authorized users. The framework helps to have automated access reviews in which administrators can certify roles and permissions regularly.

5. Scalability and Flexibility

Healthcare organizations are perceived as dynamic environments, where new roles, users, and data continue to be introduced regularly. The RBAC framework, therefore, should be structured in a way that it will be scalable and it will be able to support the increasing healthcare organizations and at the same time, preserve security and efficiency.

The framework takes advantage of the flexible nature of the SharePoint architecture to make sure that the RBAC system will be able to scale with the expansion of the organization. New permissions and roles are always added when necessary and the system can be extended to add more data repositories or other healthcare systems.

Moreover, the framework must be flexible and capable of adapting to any changes that take place in the healthcare sector, including new healthcare regulations or the necessity to allow new technologies to be used like telemedicine and mobile health apps.

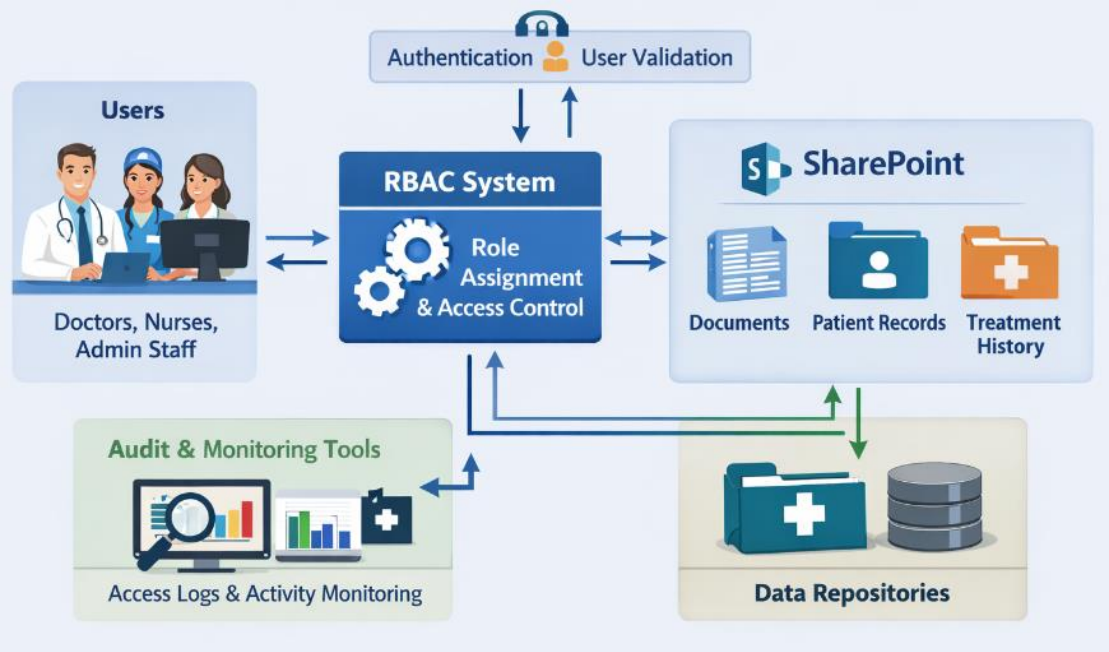

Figure 4: Healthcare RBAC System Integration with SharePoint

The proposed RBAC medical data management model with SharePoint is a flexible and scalable solution with comprehensive and detailed access control of sensitive patient information. The framework provides security of patient data by specifying the tasks, managing access, and following the mandatory healthcare policies, only authorized staff may access this data, and it is not subject to lawsuits. The system is also powerful as it integrates effective authentication, auditing capabilities, and contextual controls, which enhance the system and make it an appropriate tool in cases where healthcare institutions aim to protect patient information as well as enhance operational efficiency.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

IV. EVALUATION OF THE FRAMEWORK FOR IMPLEMENTING ROLE-BASED ACCESS CONTROL (RBAC) IN HEALTHCARE DATA MANAGEMENT USING SHAREPOINT

The analysis of the suggested Role-Based Access Control (RBAC) framework of the healthcare data management based on the SharePoint is to determine the success in the framework facilitating the healthcare data safety, increasing its regulatory adherence, and providing the healthcare professionals with the convenience of its implementation. In this section, the framework has been critically analysed on the basis of its performance in the major aspects including security, scalability, usability, compliance, and general efficiency of the system.

1. Security and Data Protection

The increased safety of healthcare data is also one of the key purposes of the RBAC framework since sensitive information is available to only authorized users. The advantage of the framework is that it enables one to allocate permissions according to user roles thus ensuring that the threat of unauthorized access is significantly reduced. The framework complies with the principle of least privilege, which is essential to patient privacy and the protection of personal health information (PHI) since the healthcare professionals and staff can access only the data they require to perform their duties.

SharePoint has built-in security capabilities, including Access Control Lists and permission inheritance, which are integrated to increase the security position of the framework. The fines-grained access control further allows an administrator to establish the access to data at a different level (site, library, document) of a SharePoint to further ensure that sensitive data is secured. Also, it has multi-factor authentication (MFA) support, which is an added benefit of increased security as it is much harder to harm the system without authorization.

But although the framework has good security mechanisms, it is requiring that it is well configured and monitored regularly to be effective. The vulnerabilities might arise due to any misconfiguration of roles, permissions, or user access to the information which may lead to data insecurity. Therefore, healthcare organizations have to make sure that the roles and permissions are audited regularly to counter possible security loopholes.

2. Scalability and Flexibility

Scalability of the framework is one more important aspect in the assessment of the framework, since healthcare organizations tend to expand with time, and new roles, users, and data are introduced. RBAC framework can support this growth and provide the flexibility of adding new roles and dealing with the complex requirements of access control.

The architecture of SharePoint allows the creation of new sites and libraries in order to handle the growing volumes of data, and the system of RBAC can be scaled by adding new role definitions and permissions to the new data sets. This scalability is especially useful with big healthcare organizations, e.g. hospitals and healthcare networks, that might have thousands of users with varying access requirements.

In addition, the hierarchical nature of the RBAC model that the framework is based on can be used to create senior and junior positions, managing the large team with more or less responsibility. As the organization grows, the structure can be easily modified to include new user groups or departments that would make sure that every user is granted the right access without overworking the system.

Nevertheless, the framework scalability could be faced with difficulties in case the healthcare organization has multi-sites or in case the regulatory demands are always subject to changes. In this instance, the framework should be regularly revised so that it is in the same direction as the changing demands and requirements.

3. Usability and User Experience

Time is an important factor in a healthcare setting and it is here that the user experience contributes to the success of an RBAC system. The framework will balance between a high level of security and ease of use so that the health professionals can easily access the information they require without undergoing unwarranted delays and complexities.

Integration of the user interface (UI) of SharePoint with the system of RBAC enables medical professionals to open documents and records in a comfortable setting. Also, the role-based permission made is user-friendly and the user only sees the data that they are allowed to view. This reduces the chances of the data overload and assists users to navigate through SharePoint without confusion.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

Moreover, application of single sign-on (SSO) and multi-factor authentication (MFA) makes authentication easy, which lowers the level of frustration which health workers experience when logging in. Although these characteristics make the system more secure, they also assist in a smooth user experience, meaning that the healthcare professionals are able to access the platform fast without going through the same authentication procedure a few times.

However, one may affect the usability of this framework when the healthcare organizations cannot define the roles and permissions clear or when the users are not properly trained on how to use the system. In this situation, users can have trouble with access to the necessary data itself or they can be overloaded with excessively complicated security measures.

4. Compliance with Regulatory Standards

Adherence to the regulations of healthcare including HIPAA, GDPR, and others is a major issue of healthcare organizations. In particular, the RBAC framework is aimed at making sure that compliance is achieved by stationing stringent access control provisions, which is essential to protecting patient information and legal requirements.

The role-based permissions in the framework allow organizations to adhere to the data minimization principle of privacy regulations because only authorized personnel are allowed to access particular types of healthcare data. Also, the auditing and logging capabilities of SharePoint, which are part of the RBAC system, enable healthcare organizations to have a precise file on who accessed what data and when, which is one of the more significant compliance requirements.

The periodic access reviews and certifications incorporated in the framework, make sure that the permissions of users are constantly reviewed and updated to comply with the regulations. This is a characteristic that contributes towards deterring unauthorized user access and also makes healthcare organizations safeguarded in line with changing regulatory demands.

Nevertheless, to achieve full compliance, continuous monitoring and modification is needed especially when new regulations are introduced or old ones revised. It is the responsibility of healthcare organizations to keep the access policies under constant review and to keep a current awareness of the regulatory environment to prevent the occurrence of compliance gaps.

5. System Efficiency and Performance

The incorporation of the RBAC structure into the SharePoint system creates a rather efficient network that enables to manage the access control centrally. The application of such native features of SharePoint like content libraries, document management, and version control makes sure that healthcare organizations can operate large amounts of data without putting pressure on the performance of the system.

Since most organizations including the healthcare have already established SharePoint, the system in question is usually stable and reliable in its performance. The RBAC model improves administrative savings in system efficiency, as it lessens the administrative overhead in case of user access control. Roles can also be defined once and allocated to users instead of administrators assigning permissions to each user individually making the task easier and also making the system uniform.

Nevertheless, similar to any infrastructure that deals with sensitive information, the framework performance can be influenced in case the underlying infrastructure is not properly managed, or the framework is not designed to run on a large scale. The healthcare organizations ought to invest in the provision of the hardware and network resource to accommodate the magnitude of the RBAC framework as it continues to grow.

RBAC framework of healthcare data management on SharePoint is a strong and efficient tool that can be used to control access of sensitive healthcare information by users. It is outstanding in the provision of powerful security controls, the ability to meet the requirements of regulatory measures, and scalability to meet the rising demands of healthcare organizations. The structure is also good in terms of striking a balance between usability and security, hence it is suitable in time constrained healthcare settings.

Nonetheless, the success of it depends on the correct implementation, configuration and continuous monitoring. To prevent security breaches, healthcare organizations have to make sure that roles and permissions are clearly understood, user authentication is strong, and the regulatory standards are observed. Although the framework is very scalable,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 2, March-April 2023 |

DOI:10.15662/IJEETR.2023.0502010

organizations should also be ready to resolve problems created by dynamic user roles, changing regulations and incorporation of new technologies. Altogether, the given RBAC framework is a thorough solution to the problem of the security and efficient access to healthcare data in SharePoint.

V. CONCLUSION AND FUTURE WORK

To sum up, Role-Based Access Control (RBAC) framework of healthcare data management with the help of SharePoint is a complex solution to the protection of sensitive healthcare data, compliance with the regulations, and efficiency of operations. The assigning of particular roles to the users and restricting their access to the healthcare data on the basis of their roles increases the data security, reduces the chances of unauthorized access, and complies with the major privacy regulations like the HIPAA and GDPR. The combination of the native security capabilities of the SharePoint platform, along with the excellent authentication capabilities and fine-grained access control, can be used to ensure that the data required by authorized personnel is accessed by them, which, in turn, will enhance patient privacy and enhance the workflow of the organization.

Moreover, the scalability and flexibility of the framework enable healthcare organizations to adapt to evolving need, such as adding additional staff or starting the process of adding new systems or modifying the regulatory compliance. The design of the system is user-friendly, and the fact is that healthcare workers can obtain the required data rather fast without interfering with the security and performance.

Nonetheless, similar to any complicated access control mechanism, the success of the framework relies on incessant tracking, frequent assessments of access, and appropriate setup. Healthcare organizations have to make sure that roles, permissions, and data access policies are constantly updated and in accordance with the changing standards.

Research on this framework is valuable in the future by incorporating greater flexibility and efficiency to the framework in difficult settings of healthcare. The possible improvement area could be the implementation of sophisticated technologies, including machine learning, to dynamically allocate roles or identify abnormalities in user activities that might suggest the attempts of unauthorized access. The framework can be as well extended to serve mobile health applications and remote healthcare services, which is an important aspect in the newly developed healthcare set-ups.

The other field where future studies will focus is the combination of the framework with the newest technologies such as blockchain to make healthcare data more secure and unalterable. In addition, ongoing enhancements of user experience, e.g. optimizing the authentication process or developing user-friendly interfaces will be critical to ensuring the balance between usability and security.

REFERENCES

[1] Microsoft, "Authorization, Users, Groups & RBAC in SharePoint," Microsoft Learn, [Online]. Available: https://learn.microsoft.com/en-us/sharepoint/dev/general-development/authorization-users-groups-and-the-object-model-in-sharepoint.
[2] M. R. SharePoint, "Role-Based Access Control in SharePoint Online," [Online]. Available: https://www.mrsharepoint.com/role-based-access-control/.
[3] Reco.ai, "SharePoint Security Best Practices for Data Protection," [Online]. Available: https://www.reco.ai/hub/sharepoint-security-best-practices.
[4] M. D. P. I. (MDPI), "Enhancing Healthcare Security: Unified RBAC/ABAC Model," *MDPI*, vol. 17, no. 6, p. 262, 2021. [Online]. Available: https://www.mdpi.com/1999-5903/17/6/262.
[5] HealthManagement.org, "Ensuring Secure Access to Health Data with Role-Based Access Controls," *HealthManagement.org*, [Online]. Available: https://healthmanagement.org/c/cybersecurity/News/ensuring-secure-access-to-health-data-with-role-based-access-controls.
[6] M365Corner, "What is Role-Based Access Control in Microsoft 365?" [Online]. Available: https://m365corner.com/m365-glossary/role-based-access-control.html.
[7] Cabot Solutions, "RBAC for Secure Healthcare SaaS Applications," *Cabot Solutions*, [Online]. Available: https://www.cabotsolutions.com/blog/role-based-access-control-rbac-for-secure-healthcare-saas-applications.
[8] Enter.Health, "Role-Based Access Control in Healthcare RCM," *Enter.Health*, [Online]. Available: https://www.enter.health/post/role-based-access-control-healthcare-rcm.