Document Management System

1. Document Management Systems in Health Insurance

A document management system is preferrable for paper records because of reasons such as being ecologically and economically beneficial, working on the records is easier, better privacy on documents by configuring authorization, protecting documents, and easier document retrieval. A document management system should let users add documents. When this system takes place in health insurance context, added documents should be related to claims and person. A claim needs access to a person’s medical files such as lab results, videos, x-rays, diagnostic reports, prescriptions and procedures. All of these data should be kept in database and better be partitioned as it allows high scalability as the amount of claims increase. A repository can also be used to collect all the required information from each database using the claim information. When the model needs to be enhanced, these partitioned storage units can be separated for example by location and these database repositories would know where to find information, making retrieval of data a lot easier. A web based platform to edit fetched documents is important because it means that a document can be altered without needing to be extracted from the system. This is especially useful to protect the integrity of documents. As these files are highly personal, privacy is a very important issue and must fit regulations. The authorization system can satisfy these requirements by assigning permissions to users to control access to the sensitive data. To protect documents, edit and scan them, the document management system will require three modules, document scanning, document editing and integrity check engine. These modules will create documents and let users work on them, while checking versions to prevent corruption of documents. An application administration module has to be implemented in a document management system by default to add users or manage the administrative operations in the system. Additionally, a user management module will be present so that users can work with their required permissions based on their user information such as password, username, and session for authentication. Additional to these modules, a separate login module will be required to authenticate users. Once the essential modules of the document management system are decided, the critical ones can be replicated. A backup of login system and document management module can be made to make the system working if one of these modules fail. An additional login module is also useful when it is given to a load balancer to distribute the workload on login module.

References:

Ismael, A., & Okumus, I. (2017). Design and implementation of an electronic document management system. Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi, 1(1), 9-17.

Haryanti, T. (2020, April). Document Management System and Reminder using SMS Gateway. In IOP Conference Series: Earth and Environmental Science (Vol. 469, No. 1, p. 012088). IOP Publishing.

Rosa, A. T. R., Pustokhina, I. V., Lydia, E. L., Shankar, K., & Huda, M. (2019). Concept of electronic document management system (EDMS) as an efficient tool for storing document. Journal of Critical Reviews, 6(5), 85-90.

Salomi, M. J. A., & Maciel, R. F. (2017). Document management and process automation in a paperless healthcare institution. Technology and Investment, 8(3), 167-178.

Tummers, J., Tobi, H., Catal, C., &amp; Tekinerdogan, B. (2021). Designing a reference architecture for Health Information Systems. BMC Medical Informatics and Decision Making, 21(1). <https://doi.org/10.1186/s12911-021-01570-2>

Zhao, W., Durkalski, V., Pauls, K., Dillon, C., Kim, J., Kolk, D., Silbergleit, R., Stevenson, V., &amp; Palesch, Y. (2010). An electronic regulatory document management system for a clinical trial network. Contemporary Clinical Trials, 31(1), 27–33. https://doi.org/10.1016/j.cct.2009.09.005

1. Document Management System Design

Diagram

Description automatically generated

The system starts with login. There are two identical systems that have the same copy of database. A load balancer is attached to either login component to handle massive amount of clients. After the authentication from the login component, the web server processes the request of the client. There is a backup web server component to keep the system working if the main web server fails. An administration level access can reach directly to these web servers to carry out administrative processes. The requests are computed in the document management server. The server has document adding, editing and integrity check engine modules to add and change documents without corrupting the originals. Application administration module is to compute administrative operations. User management component handles generic functions of user management. Workflow component operates on the information from the user to create new claims or let the employees review older claims. Finally, access and authorization module check user access level to carry out the operations required and reach certain documents. As this is the logic of the whole system, there is a backup server in case this one fails. DB Repository is a virtual server that receives the request of which documents are required or will be saved. For example, if an insurance invoice is requested then the repository would fetch all the documents related to that invoice and return them to the document management server. A backup for the repository exists if this one fails. Finally, the storage is partitioned to hold different types of documents.

1. The system starts with handling as much as login requests the system can bare. Therefore, the first bottleneck would be the web server, handling all the requests. As there is a backup web server, it would be easy to eliminate this potential bottleneck with a load balancer. The same goes for the DB repository as well. Finally, as there is also the replication of the main logic, document management server, the system is highly reliable against single point failures.
2. The document data is partitioned to make the storage scalable. If sharding is applied for partitioned, that would increase the scalability even further. The load balancer also contributes to the scalability with replicated login components.
3. Privacy and security are managed with authentication and authorization. The users have to be recognized and have the right permission to access data. This is highly secure as the data and logic is not accessible if the security check fails.
4. The system can be managed by a small IT team of two people. The main task is to keep the replicated modules up to date. Database skills are the most important for this one. In the future as well, as the scale of the system increases, additional management would not be required.
5. The backup servers are not kept in circulation until they are required, therefore, the system can be made green by keeping them in sleep. The login modules might be considered costly from a green computing perspective.