**Chapter One**

# **INTRODUCTION**

## **1.1 Background of the Study**

With the advancement of computer technology, electronic documentation and the use of electronic medical records have become more feasible. Medical records on a shared computer network that are read and written electronically on a relational database using a graphic user interface are referred to as electronic medical records. In the study entitled “A comparison of electronic records to paper records in mental health centers” (Tsai and Bond, 2007), they looked at three mental health facilities that had recently switched from paper to electronic medical records. Electronic records' documentation was shown to be more thorough and retrievable than paper records. As per the study, this finding can be a factor to take in when making treatment decisions.

In the study entitled “Perceived Benefits of Implementing and Using Hospital Information Systems and Electronic Medical Records” (Khalifa, 2018), they pointed out six ways EMRs could enable data accessibility and care organization: improving access to data during patient encounters, improving processes workflow, managing information overflow to clinicians, enhancing medical decision-making process care plans, supporting operational processes and improving financial data accessibility. They also emphasized that when a computer was used to retrieve patient information, physicians earned higher overall patient satisfaction rates, and when a computer was used to enter patient information, physicians received identical satisfaction rates.

The current technological advancements in the Philippines has yet to be manifested in its healthcare system. Though there were efforts from the government to adopt various modern tools, we are still miles behind other countries. On a study entitled “Barriers to the Adoption of Electronic Medical Records in Select Philippine Hospitals: A Case Study Approach” (Ebardo and Celis, 2019), identified barriers such as weak infrastructure, technology complexity and poor interface design of applications have made it difficult for various health organization to progress. Another study entitled “Barriers to Electronic Health Record System Implementation and Information Systems Resources: A Structured Review” (Gesulga et al., 2017), they determined another set of barriers to the adoption of EMRs in the Philippines namely: User resistance, lack of education and training, and concerns arising from data security. In a paper entitled “Identifying Healthcare Information Systems Enablers in a Developing Economy” (Ebardo and Tuazon, 2019), they discussed how the integration of existing information systems to be “paper-less” can produce potential savings. This is crucial given that the Philippines is still a developing country and has budget constraints to health systems.

The current pandemic situation poses another scenario for the state of EMRs in our country. Government has boosted efforts in immunizing majority of the population. Local Government Units (LGUs) had implemented varying strategies to keep proof and records of vaccinations. Areas inside the National Capital Region (NCR) have setup online web application to accommodate the vaccination process. Specifically, the city of Manila had employed a digitized way of keeping vaccination certificates and making them downloadable to its citizens. Other cities like Quezon City and Makati have a hybrid of online and manual processes. Although NCR cities have initiated the computerized way of the vaccination process, it is worth noting that majority of the Philippines (especially on province and remote areas) still utilize the pen and paper route.

## **1.2 Statement Problem**

At present, there is no unified system being implemented in the Philippines on Vaccination Certificates. Local Government Units (LGUs) have different strategies on their issuance of vaccination certificates. Most of them issue paper-based cards while some LGUs have web applications for their constituents to access the records. Security of these records is also in question as there are reports of people having tampered certificates to be used on various purposes. A news article from Philstar dated July 23, 2021 reports local LGUs warning the public against fake COVID-19 Vaccination cards.

## **1.3 Objectives of the Study**

This study aims to design and develop an application that will integrate blockchain and IPFS to ensure the integrity of vaccination data.

Specifically, the study seeks to address the following objectives:

1. To apply concept of Merkle DAG and Keccak Hash Algorithm for data storage.
2. To apply Proof of Authority (PoA) blockchain in maintaining transactional records.
3. To validate security aspects of the proposed application by using Solidity Security Audits based from Smart Contract Weakness Classification Registry (SWC Registry). The security audits namely:
   1. Securify (Trail of Bits)
   2. Slither (Chain Security)

## **1.4 Scope and Limitations**

The study will be focusing on developing an application for management of COVID-related records. Since there are privacy regulations concerning health information, the researcher will use dummy data and instead will probe more on the processes on how these records are archived or managed.

The study will exclude vaccine management such as scheduling. Thus, it will be focused on the results or outputs of these processes. The study assumes that information from the vaccine transaction are ready to be encoded in the system.

The study will only be concerned on Vaccine Certificates. The researcher will concentrate on developing an alternative storage system and accessibility strategy for medical units, patients and other verifying party.

## **1.5 Significance of the Study**

Results obtained from the study will benefit the following stakeholders:

**Patients**. Above all, patients will greatly benefit on this application. Various regulations and laws have been implemented to ensure people are not spreaders or vaccinated. Currently, there are no unified way in getting and presenting these records are proof. More so, bad actors are using this pandemic to make money out of tampering records. The application will help solve the woes of patients in terms on ease of access and portability of their records. They will also have full autonomy of said records.

**Medical Personnel**. The application will help medical workers to focus on their medical line of duty and alleviating various admin jobs.

**Third Party Validators.** As mentioned above, records tampering has become rampant. Businesses or employers requiring such records can now be protected of this illegal activity.

## **1.6 Definition of Terms**

**Cipher text** - A series of randomized letters and numbers which humans cannot make any sense of.

**Content addressing** - A way to find data in a network using its content rather than its location.

**Content Identifier (CID)** - A label used to point to material in IPFS. It doesn't indicate where the content is stored, but it forms a kind of address based on the content itself. CIDs are short, regardless of the size of their underlying content.

**Cryptography** - Science of secret writing with the intention of keeping the data secret.

**Digital Envelope** - A secure electronic data container that is used to protect a message through encryption and data authentication.

**Digital Signature** - A cryptographic value that is calculated from the data and a secret key known only by the signer.

**Distributed Hash Table (DHT)** - A decentralized data store that looks up data based on key-value pairs.

**Hash Digest** - Output of the hash function.

**Hashing** - Process that calculates a fixed-size bit string value from a file.

**Hash Table** - A type of data structure that stores key-value pairs. The key is sent to a hash function that performs arithmetic operations on it.

**InterPlanetary File System (IPFS)** - A protocol and peer-to-peer network for storing and sharing data in a distributed file system.

**Peer-to-Peer (P2P) Network** - A group of computers are linked together with equal permissions and responsibilities for processing data.

**Plain Text** - Clear, basic unencrypted string of text.

**Private Key** - Used to decrypt cipher text to plain text and only available to its owner.

**Public Key** - Used to encrypt plain text to cipher text and available to anyone accessing the application.