Most of the modern health-related information is collected, maintained, and accessed through computerized systems. However, the interaction with this information needs to comply with the US federal regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to the complexity of healthcare regulations, it’s not easy to deploy a compliant system, especially for heterogeneous systems designed to allow data transfer and communication. Web services can be used to solve the problem of incompatible systems intercommunication; however, a generic model for HIPAA enforcement is required. In this paper we propose a generic HIPAA complaint privacy access control model for web services that can be easily applied to any existing covered entity web services.

**Purpose of the Study**

- Evaluate the requirements and the components that should be available in a privacy preserving HIPAA-compliant access control model for web services.
- Specify the criteria for formalizing HIPAA.
- Find the features required in an access control language to express the formalized rules.
- Create a web service model prototype and that implements the access control model.

**Abstract**

Most of the modern health-related information is collected, maintained, and accessed through computerized systems. However, the interaction with this information needs to comply with the US federal regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to the complexity of healthcare regulations, it’s not easy to deploy a compliant system, especially for heterogeneous systems designed to allow data transfer and communication. Web services can be used to solve the problem of incompatible systems intercommunication; however, a generic model for HIPAA enforcement is required. In this paper we propose a generic HIPAA complaint privacy access control model for web services that can be easily applied to any existing covered entity web services.

**HIPAA Overview**

- Health Insurance Portability and Accountability Act (HIPAA). Also know as Public Law 104-191.
- Passed by the U.S. Congress on August 996.
- Privacy laws are specified in Title 2. Preventing health care fraud and abuse (administrative simplification), which includes: transactions and code sets; identifiers; privacy; and security. The concentration of this work will be on the privacy section of the law, more specifically, section 164.
- Very complex and dense, hard to use as a guide by software developers.

**HIPAA Formalization Criteria**

Any formalization should be:

- Complete and cover all the privacy rules in HIPAA.
- Context-based: Extract any law context including the roles, purposes, etc.
- Exception handling: handle the rule itself and any exception to the rule

**Access Control language**

Apply the formalized rules to form an access control that can handle any request formatted as:

```
```

**Web Services**

- Software system designed to support interoperable application-to-application interaction over a network.
- Web services utilize a set of eXtensible Markup Language (XML)

![Fig. 1. Web service conceptual and implementation models mapping](image)

**Model Prototype**

- [Purpose]
- [Data User]
- [Condition]
- [Operation]
- [Data Type]
- [Obligation]

**Conclusion and Future Work**

- Create a prototype of the proposed privacy access control model.
- Pointed out the model components and each component requirements.
- Still need to carry out an extensive detailed research for each component.
- Put all the pieces together to implement the proposed model.

**References**