VITL

Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Introduction

Introduction

This set of information security policies is designed to provide the foundation for the information security program and practices necessary to protect the confidential information of Vermont Information Technology Leaders (VITL).

The policies are organized into four basic policies, by type of policy, each with multiple sections to deal with specific issues.

1) **The Information Privacy and Security Management Process Policy** provides the basis for the ongoing processes that must be in place for HIPAA compliance and good privacy and security, including such items as designation of a privacy and security officer, risk assessment and analysis, evaluation, audits, reviews, training, and documentation. Also included are the requirements for being able to survive and recover from a variety of information threats and disasters.

2) **The Information System User Policy** includes all of the information that a VITL staff member would need to know in order to work securely, such as how to get access to systems and networks, what are user rights and acceptable use, how to handle portable devices, remote access, and what the user should do if there is a security incident.

3) **The Information System Access Control Policy** provides for the technical and physical management of access to information held by VITL, by the use of authentication, perimeter security, encryption, physical access control, and secure management and disposal of data.

4) **The Information Security Incident Response Policy** stands alone as a policy, so that it is easily referenced and used in the sometimes-stressful environment surrounding incidents and potential breaches.

The policies are designed to work together with minimum overlap, and all policies are expected to have additional procedures defined in support of the policies and procedures included here. It is hoped that these policies are not often modified, but are supplemented by new procedures as necessary. Procedures are provided separately for policies 1 and 3, while procedures are integrated into policies 2 and 4, to ensure easy access by the general user, and in the event of an incident.

These policies, once implemented, should be reviewed at least annually and updated as necessary.