Protected Health Information Privacy Policy

Implemented: April 14, 2003

I. PURPOSE STATEMENT

The following privacy policy is adopted to ensure that the State of South Dakota's Bureau of Information and Telecommunications (Bureau) complies fully with all federal and state privacy protection laws and regulations. Protection of an individual's privacy is of paramount importance to this organization. Violations of any of these provisions will result in disciplinary action.

II. ASSIGNING PRIVACY AND SECURITY RESPONSIBILITIES

Specific individuals within the Bureau's workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy and Security Rule's requirements. Furthermore, these individuals will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum, there will be one individual designated as the Privacy Officer and one individual designated as the Security Officer.

III. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

The Bureau maintains the policy that protected health information may not be used or disclosed except by authorized state agencies' employees.

IV. NOTICE OF PRIVACY PRACTICES

It is the Bureau's policy that the Protected Health Information Privacy Policy Statement must be published, that any revisions to it be provided to all appropriate state agency staff at the earliest practicable time, and that all uses and disclosures of protected health information are done in accordance with the Bureau's Protected Health Information Privacy Policy Statement.

V. DISCLOSURE OF PROTECTED HEALTH INFORMATION

All disclosures of protected health information must be limited to the appropriate state agency personnel.

VI. ACCESS TO PROTECTED HEALTH

Access to protected health information must be granted to each employee or contractor based on the assigned job functions of the employee or contractor. Also, such access privileges should not exceed those necessary to accomplish the assigned job function.

VII. COMPLAINTS

All complaints relating to the protection of health information will be investigated and resolved in a timely fashion. Furthermore, all complaints will be addressed to the Bureau's Privacy Officer, who with the appropriate Bureau manager, will be duly authorized to investigate complaints and implement

resolutions if the complaint stems from a valid area of non-compliance with the HIPAA Privacy and Security Rule.

VIII. PROHIBITED ACTIVITIES

No employee or contractor may engage in any intimidating or retaliatory acts against any individual who files a complaint or otherwise exercises their rights under HIPAA regulations.

IX. RESPONSIBILITY

The responsibility for designing and implementing procedures to implement this policy lies with the Bureau's Privacy Officer.

X. VERIFICATION OF IDENTITY

The identity of all persons who request access to protected health information will be verified before such access is granted.

XI. MITIGATION

The effects of any unauthorized use or disclosure of protected health information will be mitigated to the extent possible.

XII. SAFEGUARDS

Appropriate physical safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy and Security Rule. These safeguards will include physical protection of the premises and protected health information, technical protection of protected health information maintained electronically, and administrative protection. Administrative and technical safeguards will be imposed when employees leave positions in the Bureau. Such safeguards will include:

1. Retrieval of keys or security access cards.

2. Discontinuation of computer access codes or passwords.

XIII. BUSINESS ASSOCIATES

Business associates will be contractually bound to protect health information to the same degree as set forth in this policy. It is also the Bureau's policy that business associates who violate their agreement will be dealt with first by an attempt to correct the problem and, if that fails, by termination of the agreement and discontinuation of the business associate's services.

XIV. TRAINING AND AWARENESS

All members of our workforce will be trained on the policies and procedures governing protected health information as well as how the Bureau complies with the HIPAA Privacy and Security Rule. New

members of our workforce will receive training on these matters within a reasonable time after they have joined the workforce. It is the Bureau's policy to provide training should any policy or procedure related to the HIPAA Privacy and Security Rule materially change. We will provide this training within a reasonable time after the policy or procedure materially changes. The Bureau will document the training provided. Documentation will include the names of the participants, the date of the training, and the subject matter covered.

XV. SANCTIONS

Sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies.

XVI. RETENTION OF RECORDS

The Bureau will retain the HIPAA privacy rule records for a period of six years. Records required to be retained under the HIPAA Privacy and Security Rule will be maintained in a manner that allows for access within a reasonable period of time. The record retention time requirement may be extended at the Bureau's discretion to meet with other governmental regulations or to address other governmental operations or functions.

XVII. COOPERATION WITH PRIVACY OVERSIGHT AUTHORITIES

Oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services will be given full support and cooperation in their efforts to ensure the protection of health information within this organization. In addition, all personnel must cooperate fully with all privacy compliance reviews and investigations.