Confidentiality Policy

Pennsylvania Statewide Immunization Information System (PA-SIIS)

Pennsylvania Department of Health (Department)

Purpose: To ensure the confidentiality of information in PA-SIIS.

Responsibility: All PA-SIIS Users and PA-SIIS Staff

Definition: **Confidentiality** is the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are unnecessary and unlawful.

Background

The PA-SIIS is a statewide immunization registry and tracking system that serves the public health goal of reducing or eliminating vaccine preventable diseases. The PA-SIIS was developed to achieve complete and timely immunizations of individuals. A major barrier to reaching this goal is the continuing difficulty of keeping immunization records accurate and up to date. The PA-SIIS addresses this problem by collecting immunization information from public and private health care providers; linking an individual immunization record from different provider practices; and merging that immunization information from different providers to create a complete, accurate and current record. This assists health care providers to appropriately immunize all patients in their care.

This policy ensures the information maintained within the PA-SIIS is kept confidential by allowing participating health care providers to have access to patient information within specific guidelines. Clarification regarding policy procedures are explained below.

I. Agreement to Protect Confidentiality

The PA-SIIS has a variety of user access levels, dependent upon job responsibility. As an example, the PA-SIIS staff can access all information, whereas provider sites have limited access. The PA-SIIS staff, all users of the PA-SIIS and their immediate supervisors must sign the User Agreement

Acknowledgement prior to system use. A signature on the User Agreement Acknowledgement indicates that the user has read this policy, understands the content, and agrees to abide by its terms. The initial signed User Agreement Acknowledgement is on file by the PA-SIIS, however, Agreements are electronically renewed annually. The immediate supervisor or the owner of the provider practice is required to notify the PA-SIIS as soon as possible of any user account that requires termination due to an employee resignation or change in job responsibilities that no longer requires access to the PA-SIIS.

Inappropriate access of records is strictly prohibited. Violation of the User Agreement Acknowledgement results in system use termination. In addition, the user's supervisor and the owner of the provider practice will be notified of the breach of confidentiality and asked to take action appropriate to their organization.

II. Notification

All participating provider practices, with the exception of those operating on behalf of the Department, must notify patients that their information will be included in the PA-SIIS. The Department is a public health authority legally authorized to receive information without patient authorization for the purpose of preventing or controlling disease. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule states that providers may disclose protected health information to public health authorities for public health activities without authorization from the individual. These public health activities include preventing or controlling disease, injury, or disability; reporting disease, injury and vital events such as birth or death; and conducting public health surveillance, public health investigations and public health interventions according to the [45 CFR 164.512(b) and Disease Prevention and Control Law, 35 P.S. §521.1, et seq., and the regulations promulgated thereunder, 28 Pa. Code §27.1 et seq. (relating to communicable and noncommunicable diseases)]".

III. Use of Immunization Registry Data

The purpose of the PA-SIIS is to assist in deterring vaccine preventable diseases by collecting and tracking immunization histories through a shared network. The PA-SIIS users are expected to access, modify, and update the registry data (immunization histories and individual demographics) only for needs related to this intended purpose. The PA-SIIS users and the PA-

SIIS staff must make every reasonable effort to ensure that the immunization information is not used to harm any individual (e.g., to deny services or to track immigration status). The PA-SIIS staff and the PA-SIIS users **may not** under any circumstances:

- Reveal or share any records or immunization data except in the course of official authorized duties, such as accessing, modifying, and updating PA-SIIS records without proper authorization.
- Examine or read any records or immunization data regarding family, friends, public figures, celebrities, etc. except on a "need-to-know" basis.
- Access the PA-SIIS outside of the job site.
- Discuss or reveal the content of records or the immunization data with any person unless both persons have the authority to know the information.
- Discriminate against, abuse or take any adverse action toward a person to whom the record or immunization data pertains.
- Compile any aggregate data or statistics from the PA-SIIS except as needed to complete assigned tasks and duties.
- Contact a person whose immunization record is part of the PA-SIIS except on official business or in the course of official duties without proper authorization from the PA-SIIS.

The penalties for a breach of confidentiality are outlined in section V: Penalties for Unauthorized Disclosures.

IV. Access to and Disclosure of Registry Information

All the data stored within the PA-SIIS is held in strictest confidence. The PA-SIIS staffs work closely with attorneys in the Department as well as the Centers for Disease Control and Prevention to ensure that all policies adopted for the PA-SIIS are in full compliance with all applicable state and federal laws and regulations. The PA-SIIS is property of the Pennsylvania Department of Health. The PA-SIIS data is accessible only to authorized persons who have signed a User Agreement Acknowledgement. After signing the Agreement, the PA-SIIS assigns the user an ID and a password. Sharing IDs and passwords is strictly prohibited. An individual's immunization record will be accessible to patients, parents, and/or guardians through the Primary Care Provider upon request. Aggregate immunization data, with no personal identifiers that does not compromise the confidentiality of an individual, is considered public health information and can be shared. As mentioned in Section I: Agreement to Protect Confidentiality, the web-based software has a variety of user access levels; therefore, accessing new and existing client records not applicable to a provider

site is prohibited. The web-based application keeps an ongoing log/audit trail that enables the PA-SIIS staff to track user activity within patient records and to monitor this log closely for inappropriate activity.

V. Penalties for Unauthorized Disclosures

If any inappropriate use or disclosure of immunization data is discovered, the user is warned and user privileges may be terminated, depending on the nature of the disclosure. If the user is an employee of the Department, appropriate disciplinary action and/or termination will occur. If the user is not an employee of the Department, the PA-SIIS may terminate the user's PA-SIIS access and/or may refer the matter to the administration of the provider site where the user is employed. The penalties for unauthorized disclosure(s) are as follows:

- HIPAA Privacy Rule

  - Civil penalties. Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.

  - Federal criminal penalties. There would be federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.