MEMORANDUM OF UNDERSTANDING

Policy and Procedures for Protecting Privacy, Confidentiality and Security of Individually Identifiable Information Contained in the Alabama Immunization Registry

1 PURPOSE

1.1 To ensure compliance with current Alabama legislation related to Alabama's immunization registry.

1.2 To ensure compliance with patient privacy protections legislation as outlined in the Privacy Rule, Health Insurance Portability and Accountability Act of 1996 (HIPAA).

1.3 To ensure compliance with the Privacy Act of 1974.

1.4 To ensure consistent understanding and practice among immunization providers in Alabama.

1.5 To specify formal structures.

1.6 To ensure responsibility and accountability.

1.7 To establish procedures for releasing information and assigning access privileges.

2 SCOPE

2.1 All persons who provide immunization services to children, adolescents, and adults in Alabama or who access immunization information, including but not limited to, health department employees, medical staff in public and private provider offices, contractors, and vendors.

3 RELATED DOCUMENTS

3.1 Rules of the State Board of Health, Chapter 420-6-2

3.2 The Health Insurance Portability and Accountability Act of 1996

3.3 Standards for Privacy of Individually Identifiable Health Information

3.4 The Privacy Act of 1974

3.5 The Computer Systems Center Disaster Recovery Plan

3.6 Community Immunization Registry Manual

3.7 National Immunization Program (NIP) Privacy and Confidentiality Resources

3.8 Medical Privacy Regulation, Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, United States General Accounting Office

4 DEFINITIONS

4.1 Privacy - the legal right of an individual to limit access by others to some aspect of the person (National Vaccine Advisory Committee, 1999).

4.2 Information privacy - the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967). This means that someone is under a duty either not to disclose information or to prevent unauthorized access to information by others.

4.3 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 inconsistent with the understanding of the original disclosure (National Advisory Committee, 1999).

4.4 Data Security - exists when information is protected from accidental or intentional disclosure to unauthorized persons and from unauthorized or accidental alteration (Institute of Medicine, 1991).

4.5 User - any person who is authorized to access, use, modify, read, or disclose any information contained in the immunization registry database.

4.6 Acronyms:

ADPH	Alabama Department of Public Health
ImmPRINT	Immunization Provider Registry with Internet Technology

5 RESPONSIBILITIES

5.1 Role of the ADPH

Immunization Division Directors shall:

- Provide the resources and direction necessary to support the privacy, confidentiality and security of information contained in ImmPRINT,
- Take measures to ensure adequate funding for procurement of adequate technical security mechanisms and for studying vulnerabilities and required practices,
- Revise technical and organizational policies, practices and procedures to protect identifiable information,
- Maintain an education and training program to ensure that all users of ImmPRINT receive the minimum level of training relevant in privacy and security practices and knowledge regarding existing confidentiality policies,
- Limit access to ImmPRINT data to authorized office personnel only,
- Designate an individual(s) to be responsible for seeing that the privacy procedures are adopted and followed,
- Periodically review ImmPRINT safeguards and provide policy guidance,
- Approve requests to use ImmPRINT data for research purposes. (the researcher must sign an agreement to maintain the confidentiality of all ImmPRINT data that is used), and
- Review and revise this policy as needed but not less than annually.

Computer Systems Center employees who work with ImmPRINT shall:

- Conduct formal vulnerability assessments,
- Maintain safeguards to protect against a defined threat to ImmPRINT, its resources, and its data,
- Guarantee that authorized users can access needed information in emergency situations,

- Backup immunization histories in ImmPRINT nightly so that this information can be restored or recovered from both recent and archival files if the primary data are destroyed or invalidated,

- Ensure that nightly backup tapes are stored in fireproof vaults off-site.

- Implement the Computer Systems Center Disaster Recovery Plan in cases of any type of disaster,

- Conduct auditing events periodically,

- Maintain audit trails in retrievable and usable forms,

- Review audit logs in response to requests from registry users, providers and from individual patients/parents/guardians and through more formal means such as random sampling, and

- Ensure the protection of privacy and confidentiality of ImmPRINT data if ImmPRINT data is integrated with other health information systems.

Area Immunization Managers shall:

- Assist to develop and revise training related to privacy, confidentiality and security of identifiable information, and

- Conduct training in security practices and privacy and confidentiality before any person is granted access to ImmPRINT.

Disease Intervention Specialists that work with ImmPRINT shall:

- Conduct training in security practices and privacy and confidentiality before any person is granted access to ImmPRINT,

- Assist to develop and revise training related to privacy, confidentiality and security of identifiable information, and

- Coordinate user agreement details and assign user identification codes.

5.2 Role of Public and Private Immunization Providers

Physician and Nurse Providers shall:

- Accept responsibility for the protection of registry information,

- Limit access to ImmPRINT data to authorized office personnel only,

- Ensure the protection of privacy and confidentiality of ImmPRINT data if ImmPRINT data is integrated with other health information systems,

- Ensure that patients/parents/guardians are notified of the existence of ImmPRINT and the information contained in the ImmPRINT database,

- Inform patients/parents/guardians of the purpose and potential uses of ImmPRINT,

- Inform patients/parents/guardians of the types of organizations to which identifiable or unidentifiable information is commonly released,

- Inform patients/parents/guardians of the policies and procedures in place to protect patient privacy,

- Permit patients/parents/guardians to review and change information in ImmPRINT,

- Give patients/parents/guardians the right to request audits of all accesses to their electronic immunization record and to review such logs,

- Inform patients/parents/guardians of their right to refuse to have their immunization history and other identifiable information entered into ImmPRINT and of their right to change their decision at any time, and

- Document in the medical record a patient, parent or guardians decision not to participate in ImmPRINT.

Office Managers shall:

- Train employees so that they understand the privacy procedures,

- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed,

- Ensure the protection of privacy and confidentiality of ImmPRINT data if ImmPRINT data is integrated with other health information systems,

- Limit unauthorized physical access to computer systems, displays, networks, and immunization records, and

- Establish procedures to destroy printouts of ImmPRINT immunization records that are not incorporated into the formal medical record.

6 PROCEDURAL GUIDELINES

6.1 Technical Security Mechanisms

- Unique identifiers or log-in IDs and passwords are used to authenticate or verify the identification of users and make it possible to hold users accountable for their actions.

- Every individual must have a unique identifier for use in logging onto ImmPRINT.

- Users are required to change their passwords every 60 days and to select passwords that cannot be guessed easily.

- If users attempt to access ImmPRINT from remote locations, an authentication process is required through the form of encrypted passwords.

- Audit trails record all transactions that access patient information, including the specific type of information accessed.

- Encryption is used to protect log-in IDS, passwords, databases, and all patient-identifiable information transmitted electronically.

- All patient-identifiable data is encrypted before transmission over the World Wide Web. The Web site application is secured through a Digital Certificate provided by Verisign, Inc.

- Computer workstations will log off automatically if left idle for 15 minutes.

- Users should lock their work stations each time they leave their work area.

6.2 Access Control

- Only legitimate users are granted access to ImmPRINT.

- Access control techniques such as levels of access are used to limit the types of data that an individual can read, enter, or alter and the types of functions they can perform.

- Because access to ImmPRINT entails a connection with the Internet, firewalls provide strong, centralized security and allow outside access to only those ImmPRINT functions that the user is authorized for.

- Users are restricted access to only that information for which they have a legitimate need or for which their access is justifiable. These controls are based on the job categories. Job descriptions are narrowed as much as possible to allow more control of access privileges.

- The proper balance between access and privacy will depend on the specific setting and the need to ensure access to information in emergency situations. For example, in some office settings the office manager or administrative staff is responsible for generating immunization records.

- Unauthorized personnel should not have access to the locations where ImmPRINT is being used.

7 ADDITIONAL GUIDELINES

7.1 Unidentifiable data can be used for statistical purposes or to identify high risk populations.

7.2 Providers or ImmPRINT users may disclose immunization information to the ADPH and to the ImmPRINT database without consent or authorization.

7.3 Use of ImmPRINT data in a manner that is punitive to patients/parents/guardians is prohibited. No information from ImmPRINT will be made available to law enforcement and the Immigration and Naturalization Service, except as required by law.

7.4 A patient, parent or guardian will not be penalized for choosing not to participate in ImmPRINT.

7.5 Violations of privacy, confidentiality and security can be sanctioned according to applicable federal, state and/or local law.