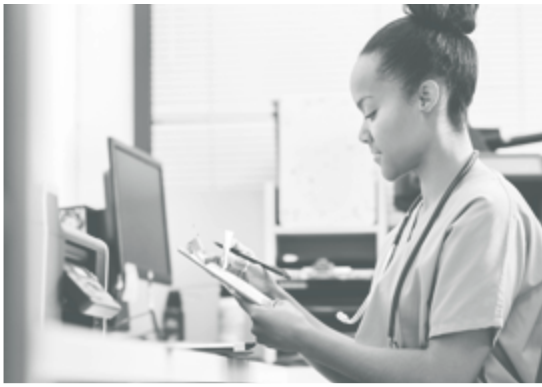
AIRA
AMERICAN IMMUNIZATION REGISTRY ASSOCIATION
Immunization Information Systems for a New Era






Confidentiality and Privacy

Considerations for Immunization Information Systems

September 2016

Executive Summary

Immunization information systems (IIS) are confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area.[1] IIS are established and operated by states, municipalities, territories and the District of Columbia under applicable state, local and territorial laws.

The purpose of capturing and consolidating immunization and demographic data in an IIS is to better support clinical practice through clinical decision support and public health through aggregate and population-based analyses. It is essential that IIS manage data in accordance with federal, state, local and territorial laws around confidentiality, but IIS should never lose sight of the critical importance of using and sharing the data they gather. IIS are rich, population-based systems that can provide great value locally and nationally through real-time analyses and effective evaluation.

The privacy of individuals whose information is contained in IIS and the confidentiality of information disclosed to and by IIS are integral parts of IIS development and use. Federal, state, local and territorial laws recognize that health information can and should be shared appropriately to support individual and population health while protecting the confidentiality of information in IIS.

In the United States there is no comprehensive federal law governing the collection and use of health information. Federal law sets a floor for the protection of the privacy of individuals with respect to certain health information. State, local and territorial laws that provide more stringent protections continue to apply. Collection and use of information by an IIS are governed by the state, local and territorial laws authorizing operation of the IIS and by more general state, local and territorial laws relating to protection of health information. Federal, state, local and territorial laws must be examined to determine what information can be collected by an IIS and how IIS information can be used and disclosed.

The Centers for Disease Control and Prevention (CDC) developed functional standards for IIS operations for 2013-2017 (Functional Standards) through a consensus process. The Functional Standards lay a framework for the development of IIS through 2017.[2] CDC will develop a framework for the development of IIS beyond 2018 using a similar process. CDC recognizes that information in IIS must be secure and confidential in programmatic goal 4, which requires IIS to "[p]reserve the integrity, security, availability and privacy of all personally-identifiable health and demographic data in the IIS."[2] Functional Standard 4.1 requires each IIS to have "written confidentiality and privacy practices and policies based on applicable law or regulation that protect all individuals whose data are contained in the system".[2]

This document is intended to assist IIS as they develop policies and procedures to meet legal requirements for protecting the privacy of individuals and the confidentiality of information in IIS. The paper describes the impact of major federal laws on IIS, specifically the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3,4] and the Family Educational Rights Protection Act (FERPA)[5,6], and provides considerations for topics to include in IIS confidentiality policies.

HIPAA sets national standards that form a baseline of health information privacy protections. In general, an entity covered by HIPAA may not use or disclose protected health information unless authorized by the individual who is the subject of the information or as required or permitted by a specific provision of HIPAA.

[1] http://www.cdc.gov/vaccines/programs/iis/about.html

[2] http://www.cdc.gov/vaccines/programs/iis/func-stds.html

[3] P.L. No. 104-191, 110 Stat. 1938 (1996); 42 U.S.C. § 300gg, 29 U.S.C § 1181 *et seq*. and 42 USC 1320d *et seq*., 45 C.F.R. §§ Parts 160, 162 and 164.

[4] http://www.hhs.gov/hipaa/for-professionals/index.html

[5] 20 U.S.C. § 1232g; HHS regulations at 34 C.F.R. § Part 99

[6] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA permits the use and disclosure of protected health information without authorization for treatment, payment, health care operations and public health purposes.

This document also examines the application of FERPA as it applies to IIS. In general, FERPA governs schools and requires that a parent must give consent before a school can release immunization information in an education record.

HIPAA preempts contrary state laws; however, it does not preempt more restrictive state laws. Municipal and territorial IIS should consult their own attorney to determine the impact of HIPAA on local and territorial laws. IIS should consider the applicability of state, local and territorial laws as they develop confidentiality policies. This paper provides guidance on the topics IIS should consider for inclusion in confidentially policies and procedures and federal, state, local and territorial laws to examine as IIS develop those policies and procedures.

IIS use site agreements and user agreements to ensure that each use and disclosure of IIS information complies with IIS confidentiality polices. The document discusses provisions to consider including in site and user agreements.

More detailed analysis of the application of HIPAA and FERPA to IIS is included in Appendices. Sample confidentiality policies, site agreements and user agreements are also included in Appendices.

The information in this document is not legal advice. Each IIS should contact appropriate individuals within their own agency who are responsible for interpretation and implementation of federal and state privacy and confidentiality laws.

Table of Contents

Tables and Figures

Acknowledgments

The American Immunization Registry Association (AIRA) would like to acknowledge and thank the following individuals and organizations for their support and assistance with this important project:

- The primary researcher and writer on this project: **Elaine Lowery**, Public Health Consultant
- The AIRA Board of Directors who provided input at various stages of the effort and/or reviewed and provided comment on the final guide:
  - President – **Mary Woinarowicz**, North Dakota Department of Health
  - President-Elect – **Michelle Hood**, Nebraska Department of Health and Human Services
  - Immediate Past President – **Amy Metroka**, New York City Department of Health and Mental Hygiene
  - Secretary – **Jenne McKibben**, Oregon Immunization Program
  - Treasurer – **Beth English**, Massachusetts Department of Public Health
  - Directors
    - **Megan Meldrum**, New York State Immunization Information System
    - **Kim Salisbury-Keith**, Rhode Island Department of Health
    - **Bridget Ahrens**, Vermont Immunization Registry
    - **Belinda Baker**, Washington State Immunization Information System
    - **Bhavani Sathya**, New Jersey Immunization Information System
    - **Baskar Krishnamoorthy**, Florida Department of Health IIS
    - **Kevin Dombkowski**, University of Michigan, Child Health Evaluation and Research Unit
    - **Brandy Altstadter**, Scientific Technologies Corporation
- The AIRA Staff who contributed to this document's development:
  - **Rebecca Coyle**, Executive Director
  - **Alison Chi**, Program Director
  - **Mary Beth Kurilo**, Policy and Planning Director
  - **Nichole Lambrecht**, Senior Project Manager
- Individuals that provided feedback during the external review process:
  - **Noam Arzt**, HLN
  - **Bill Brand**, Public Health Informatics Institute
  - **Michelle Hood**, Nebraska Department of Health and Human Services
  - **Therese Hoyle**, Michigan Department of Health and Human Services & Public Health Informatics Institute
  - **Gail Horlick**, CDC Office of the Associate Director for Science
  - **Marlene Lugg**, Southern California Kaiser Permanente
  - **Craig Newman**, Northrop Grumman, Supporting CDC/NCIRD/IISSB
  - **Janet Fath**, CDC Immunization Information Systems Support Branch

Chapter 1. Introduction

Immunization information systems (IIS) are confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area.[7] IIS are established and operated by states, municipalities, territories and the District of Columbia under applicable state, local and territorial laws.

At the point of clinical care, IIS provide consolidated and combined immunization records for use by a vaccination provider in determining appropriate client vaccinations. At the population level, IIS provide aggregate data on vaccinations for use in surveillance and program operations, and in guiding public health action with the goals of improving vaccination rates and reducing vaccine-preventable disease.[7]

The privacy of individuals whose information is contained in IIS and the confidentiality of information disclosed to and by IIS are integral parts of IIS development and use. Often overlapping federal, state, local and territorial laws protect the confidentiality of information in IIS. Federal, state, local and territorial laws recognize and protect the confidentiality of information in IIS, but also recognize that health data can and should be shared appropriately to support individual and population health care.

Federal initiatives aim to increase the availability and use of electronic health information to improve the health of individuals and the population as a whole. These initiatives have resulted in an increase in data submitted to IIS and in the demand for use of IIS data.

This document is intended to provide the IIS community with considerations for confidentiality procedures and policies to meet legal requirements and ethical considerations for protecting the privacy of individuals and maintaining the confidentiality of information in an IIS. Physical, technical, administrative and organizational safeguards to ensure the security of the information in an IIS are vital to implementing confidentiality of information in an IIS. A separate AIRA document will address these security safeguards, as well as policies and procedures to implement the security safeguards.

Much of the material in this document is derived from resources identified in the Resources section, including specifically the United States Health and Human Service (HHS) website for the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[8,9] the U.S. Department of Education website for guidance on the Family Educational Rights and Privacy Act (FERPA)[10,11] and the Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information, Version 2.0, April 2015 (ONC Guide).[12]

The information contained in this document is not legal advice nor should it substitute for advice provided by legal counsel. Each IIS should consult its own legal counsel to determine how federal, state, local and territorial laws affect use and disclosure of IIS information. Since federal laws provide a floor for the protection of health information, this paper examines the impact of these federal laws on confidentiality of information in IIS. This paper does not address the impact of federal, state, local and territorial laws on the security of information in IIS, but a separate AIRA paper will address security concerns. This document does not address specific state, local and territorial laws, and is not a definitive review of federal laws as they apply to specific situations. Readers are encouraged to contact appropriate individuals within their own agency who are responsible for interpretation and implementation of federal and state privacy, confidentiality and security laws.

[7] http://www.cdc.gov/vaccines/programs/iis/about.html

[8] P.L. No. 104-191, 110 Stat. 1938 (1996); 42 U.S.C. § 300gg, 29 U.S.C § 1181 *et seq*. and 42 USC 1320d *et seq*., 45 C.F.R. §§ Parts 160, 162 and 164.

[9] http://www.hhs.gov/hipaa/for-professionals/index.html

[10] 20 U.S.C. § 1232g; HHS regulations at 34 C.F.R. § Part 99

[11] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[12] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Chapter 2. Regulatory Framework

In the United States, there is no comprehensive federal law governing the collection and use of health information. Federal law (i.e., HIPAA) sets a floor for the protection of the privacy of individuals with respect to certain health information. State (as defined in HIPAA) laws with more stringent protections continue to apply. Collection and use of information by an IIS are governed by state, local and territorial laws authorizing operation of the IIS and by more general state, local and territorial laws relating to the protection of health information. Federal, state, local and territorial laws must be examined to determine what information can be collected by an IIS and how the IIS information can be used and disclosed. This section provides a high-level overview of the regulatory framework relating to privacy and confidentiality of IIS information, including the basis for many federal, state, local and territorial laws and initiatives.

Fair Information Practices

Protection of privacy and confidentiality has always been an important part of any discussion concerning collection and use of individually identifiable information, especially as electronic collection and exchange of information become more common. Fair information practices (FIPs) is a set of overarching principles that guide information confidentiality while advancing technology. See Appendix C. Fair Information Practices. FIPs are foundational to many federal, state, local and territorial laws and organizational policies.

Federal Laws and Initiatives

Privacy and confidentiality considerations for IIS information must include analysis of several federal laws. HIPAA is based on FIPs and sets a foundation for federal protection of the privacy and security of individually identifiable health information. FERPA[13] is a federal law that protects the privacy of student education records. In the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009[14] the federal government began programs to accelerate the development and adoption of health information technology. The purpose of these efforts is to enable electronic health information to be available when and where it is needed to support patient care, enhance health care quality and efficiency, and advance research and public health, while maintaining individuals' rights with respect to their information.

Table 1 below illustrates the general applicability of HIPAA, FERPA and state, local and territorial laws to use and disclosure of health information in the context of IIS.

Table 1. General applicability of HIPAA, FERPA and state, local and territorial laws to IIS information

	HIPAA	FERPA	State, local and territorial laws
Submission (disclosure) to an IIS by entities that are not schools	Yes, if the disclosure is made by an entity governed by HIPAA (i.e., a covered entity)	No	Yes
Submission (disclosure) to an IIS by schools from an education record	No	Yes	Yes
Use/disclosure by an IIS	Yes, if the IIS is a covered function of an entity governed by HIPAA (i.e., a covered entity)	No	Yes

[13] 20 U.S.C. § 1232g; 34 C.F.R. § Part 99

[14] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq*.

HIPAA Overview

HIPAA and its implementing regulations set a national baseline of health information privacy and security protections. HIPAA is implemented through a set of regulations (rules) adopted by HHS.

- The Privacy Rule[15] sets national standards for the protection of individually identifiable health information by: health plans, health care clearinghouses, and health care providers who conduct standard health care transactions electronically (CEs or CE).
- The Security Rule[16] sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.
- The Omnibus Final Rule[17] modified the HIPAA Privacy and Security Rules and finalized the Breach Notification Rule[18] as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Omnibus Final Rule[17] strengthens aspects of HIPAA privacy and security protections and addresses responsibilities of certain entities that provide certain services for CEs (business associates).
- The official version of the Privacy Rule, the Security Rule and the Breach Notification Rule are published in the Code of Federal Regulations (C.F.R.) at 45 C.F.R. §§ Part 160,[19] Part 162,[19] and Part 164.[19] All three rules are published in one document called the Combined Regulation Text.[20]

In general, the Privacy Rule provides that a CE may only use or disclose protected health information without an individual's permission if the purpose of the use or disclosure is specifically permitted or required by the Rule. The Privacy Rule permits the use and disclosure of protected health information for several purposes without express individual authorization including most disclosures to and from an IIS. See Chapter 3. HIPAA Applied to IIS section, and Appendix A. Detailed Analysis of HIPAA.

FERPA Overview

FERPA is a federal law that protects the privacy of student education records and grants rights regarding those education records. In general, personally identifiable information contained in an education record cannot be disclosed without written consent of the parents or of an eligible student. An eligible student is one who has reached the age of 18 or who is attending a postsecondary institution at any age. Once a student becomes an eligible student, the rights given his or her parents under FERPA transfer to that student. If any person under the control of a school receives information (including immunization information), it is considered to be part of the education record, which is subject to FERPA. A school can release information in education records without the consent of the parent (or eligible student) under limited circumstances:

- Directory information
- De-identified data
- Health and safety emergency

There is no exception for release of information in education records for public health purposes on a routine basis.

HITECH

In the HITECH Act, the federal government began programs to accelerate the development and adoption of health information technology. "The purpose of these efforts is to enable an interoperable learning health system—one in which electronic health information is

[15] *Standards for Privacy of Individually Identifiable Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.160_07.html, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.164_07.html

[16] *Security Standards for the Protection of Electronic Protected Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Part 160 and Subparts A and C of Part 164, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.160_07.html, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.164_07.html

[17] http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[18] *Notification in the Case of Breach of Unsecured Protected Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations, Subpart D of Part 164, https://www.gpo.gov/fdsys/pkg/C.F.R.-2011-title45-vol1/pdf/C.F.R.-2011-title45-vol1-sec164-400.pdf

[19] http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.160_07.html

[20] http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

available and can be securely and efficiently shared, when and where it is needed, to support patient-centered care, enhance health care quality and efficiency, and advance research and public health."[21] ONC laid out this vision in several documents:

- Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure[22]
- Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information[23]
- Connecting Health and Care for the Nation—A Shared Nationwide Interoperability Roadmap (the Roadmap)[24]

One of four critical pathways to achieving the interoperable health system is identified in the ONC Roadmap as: "Clarify and align federal and state privacy and security requirements that enable interoperability."[24] The ONC Roadmap recognizes that the "success of health IT and interoperability is dependent on individuals' trust that their electronic health information will be kept private and secure and that their rights related to this information will be respected."[24] The Roadmap also notes that there is a great deal of confusion about when individually identifiable information legally can be exchanged without written permission and about diverse and specialized state privacy laws.[24]

ONC provides resources for privacy and security responsibilities, such as the ONC Guide.[25]

State, Local and Territorial Laws

HIPAA preempts less restrictive state laws, however, it does not preempt more stringent state laws. HIPAA defines state as the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands and Guam. Local and territorial IIS should consult their attorney to determine the interaction of HIPAA with local and territorial laws. IIS are authorized to operate by state, local and territorial laws. Eighty-one percent of IIS operate based on direct legal authority for public health to operate the IIS while 19% operate based on general public health authority.[26] Laws authorizing operation of an IIS will often include specific provisions concerning the collection of information by the IIS and the use and disclosure of information after it is collected by the IIS.

The proliferation of security breaches and inappropriate uses of personal data in recent years has led to an expansion of the overlapping system of privacy laws, with many states adopting or considering data protection legislation.[27] State, local and territorial laws governing data privacy can take many different forms and may sometimes overlap. Types of state privacy laws that may affect collection, use and disclosure of health information, include regulation of:

- The private sector. Laws similar to HIPAA, for example, see the Minnesota Health Records Act (Minnesota 144.291 to 144.298),[28] which sets limits on the electronic exchange of health information by health care providers.
- The public sector. Data privacy laws that protect all data held by state agencies are sometimes called an acceptable use policy. An acceptable use policy is intended to help safeguard and enhance the use and disclosure of information held by a state agency by prohibiting unacceptable use and disclosure.[29]
- All health information.
- Electronic exchange of information. These laws may have been adopted as a part of laws authorizing health information exchange organizations.
- Vital records information (births, deaths, adoptions, etc.).

[21] https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

[22] https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

[23] https://www.healthit.gov/policy-researchers-implementers/nationwide-privacy-and-security-framework-electronic-exchange

[24] https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[25] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

[26] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303

[27] http://us.practicallaw.com/6-502-0467#a596299

[28] https://www.revisor.mn.gov/statutes/?id=144.291

[29] http://msa.maryland.gov/msa/intromsa/html/acceptable.html

Unlike HIPAA, some state, local and territorial laws may require an individual's written permission before disclosing particular types of individually identifiable health information for public health purposes.

A good resource for state privacy laws is Health Information and the Law,[30] a project of the George Washington University's Hirsh Health Law and Policy Program and the Robert Wood Johnson Foundation. Another resource for state laws (focusing on interoperability) is the State Health IT Policy Levers Compendium prepared by ONC.[31]

State and IIS Policies

In addition to federal, state, local and territorial laws, some entities, including health care providers and IIS, have developed their own internal policies regarding disclosure of information that may be more stringent than either federal, state, local and territorial laws.

The U.S. legal, regulatory and policy landscape for sharing health information is complicated and sometimes contradictory. While HIPAA sets a "floor" as a federal law with its implementing regulations, state, local and territorial laws and IIS policies are often more restrictive than HIPAA and vary across states and IIS.

Emergency Powers

Declaration of an emergency may affect the way that IIS information can be used and disclosed under state, local and territorial laws. An emergency declaration might affect who has access to information under what circumstances and requirements for consent or notification, among other impacts.

State, local and territorial laws vary considerably on the mechanism and effect of an emergency declaration and IIS should consult their own legal and other appropriate authorities. Each state has a mechanism that allows government officials (e.g., the governor, state public health officers, etc.) to declare a state of emergency. The declaration may have to be approved by a legislative body or other authority within some time period. Local governments may have similar authority to declare an emergency within their jurisdiction.

State, local and territorial laws establish the effect of an emergency declaration. If permitted by state, local and territorial laws the declaration may suspend or waive state, local and territorial laws. For example, during an emergency, state or local officials may be empowered to designate the IIS as the method to track emergency related vaccine inventory and/or administration with no opportunity to exercise an otherwise available option to opt-out of including the information in the IIS.

Designated federal officials can also declare emergencies, which can result in assistance to states and in modifying some regulatory requirements. HIPAA remains in effect during an emergency; however, if an emergency is declared under a particular federal law, the Secretary of the U.S. Department of Health and Human Services may waive certain sanctions for non-compliance with HIPAA.

IIS can contact emergency response officials in their jurisdiction to obtain information about: 1) legal requirements for declaring an emergency, 2) who can declare an emergency, and 3) the effect of an emergency on regulatory and programmatic responsibilities of the IIS.

[30] http://www.healthinfolaw.org/state

[31] https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations/state-hit-policy-levers-compendium

Chapter 3. Privacy and Confidentiality in IIS

The privacy of individuals whose information is contained in the IIS and the confidentiality of information disclosed to and by IIS are an integral part of IIS development and use. Recommendations addressing confidentiality issues concerning information in IIS were first developed by the CDC, the All Kids Count Program, and the National Vaccine Advisory Committee (NVAC) in the Community Immunization Registries Manual Chapter on Confidentiality, approved by NVAC in January 1997. The confidentiality chapter was updated and approved by NVAC in February 2000 and is now out of publication.

More recently, CDC developed IIS Functional Standards for 2013-2017 (Functional Standards) that lay a framework for the development of IIS through 2017.[32] CDC will develop a framework for the development of IIS beyond 2017 using a similar process. CDC recognizes that information in IIS must be secure and confidential in Functional Standards programmatic goal 4, which requires IIS to: "[p]reserve the integrity, security, availability and privacy of all personally-identifiable health and demographic data in the IIS."[32] Functional Standard 4.1 requires each IIS to have "written confidentiality and privacy practices and policies based on applicable law or regulation that protect all individuals whose data are contained in the system."[32]

As a result of several initiatives designed to achieve the federal objectives for making electronic health information increasingly available, IIS contain immunization information for large segments of the population. In 2013, IIS contained immunization records for 90% of children, 64% of adolescents and 32% of adults.[33] Increasingly, IIS are being approached to both accept data from and disclose data to non-traditional providers and others to assist in improving individual, population and public health.

At the same time that information in IIS is being accessed and used more than ever, the number of individuals affected by breaches of health information is increasing, thereby making protection of privacy and security of IIS information even more visible and important. For breaches occurring in calendar year 2012, OCR received 222 reports of breaches involving 500 or more individuals, which affected over 3 million individuals. OCR received 239 reports of these larger breaches that occurred in calendar year 2015, which affected over 100 million individuals.[34]

HIPAA Applied to IIS

Privacy Rule

This section provides an overview of the impact of the HIPAA Privacy Rule on IIS operations. See Figures 1, 2 and 3 below, for a visual representation of the information in this section. See Appendix A. Detailed Analysis of HIPAA for more detailed information on the application of the Privacy Rule to IIS operations and for citations to specific sections of the HIPAA rules.

HIPAA governs activities of CEs and their business associates. CEs are health care providers, health plans and health care clearinghouses that transmit standard transactions electronically. State and local public health agencies are not exempt from HIPAA. The entity (state agency) housing the IIS may or may not be a CE, depending on the agency structure and whether the agency housing the IIS furnishes, bills, or receives payment for health care services. Some public health agencies do not furnish, bill or receive payment for health care services and are not subject to HIPAA. The Centers for Medicaid and Medicare Services (CMS) developed tools to assist in determining if an entity is a CE.[35] The Privacy Rule permits a CE that is a single legal entity and that conducts both covered and non-covered

[32] http://www.cdc.gov/vaccines/programs/iis/func-stds.html

[33] http://www.cdc.gov/vaccines/programs/iis/annual-report-iisar/2013-data.html

[34] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[35] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf

functions to elect to be a hybrid entity. The activities that make a person or organization a CE are its covered functions. To be a hybrid entity, the CE must designate in writing its operations that perform covered functions as one or more health care components. After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A CE that does not make this designation is subject in its entirety to the Privacy Rule. Approximately 45% of IIS considered themselves to be CE under HIPAA.[36]

The Privacy Rule protects all individually identifiable health information held or transmitted by a CE or its business associate in any form. This information is called protected health information (PHI).

After determining that an entity disclosing data is subject to HIPAA, it is important to analyze each data use and disclosure separately. If the person or entity disclosing information TO an IIS is governed by HIPAA, the disclosure must be authorized by the individual who is the subject of the information disclosed, permitted by an exception to HIPPA, or HIPAA must otherwise permit or require the disclosure. One exception to the requirement of authorization is a disclosure to a public health authority authorized by law to collect or receive the information for preventing or controlling disease and to entities that have been delegated such authority. Under HIPAA an IIS is considered to be a public health authority and a person or entity governed by HIPAA is permitted to release information to the IIS without authorization. Use BY the IIS or disclosure of information FROM the IIS must be examined separately from disclosure of information to the IIS. The IIS must determine if it is governed by HIPAA and if so, whether the use or disclosure is required or permitted by HIPAA. The HIPAA public health authority exception that allows an IIS to receive information is not the same HIPAA exception that will allow an IIS to use or disclose information. All of these issues are discussed in more detail in following parts of this section and in Appendix A. Detailed Analysis of HIPAA.

CEs may only use and disclose protected health information according to Privacy Rule provisions. Under the Privacy Rule, disclosures are either required or permitted. The Privacy Rule recognizes only two required disclosures: 1) to the HHS Secretary, and 2) to the individual.

Figure 1 below illustrates authorized and required disclosures under HIPAA while Table 2 provides referenced definitions.

[36] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303.

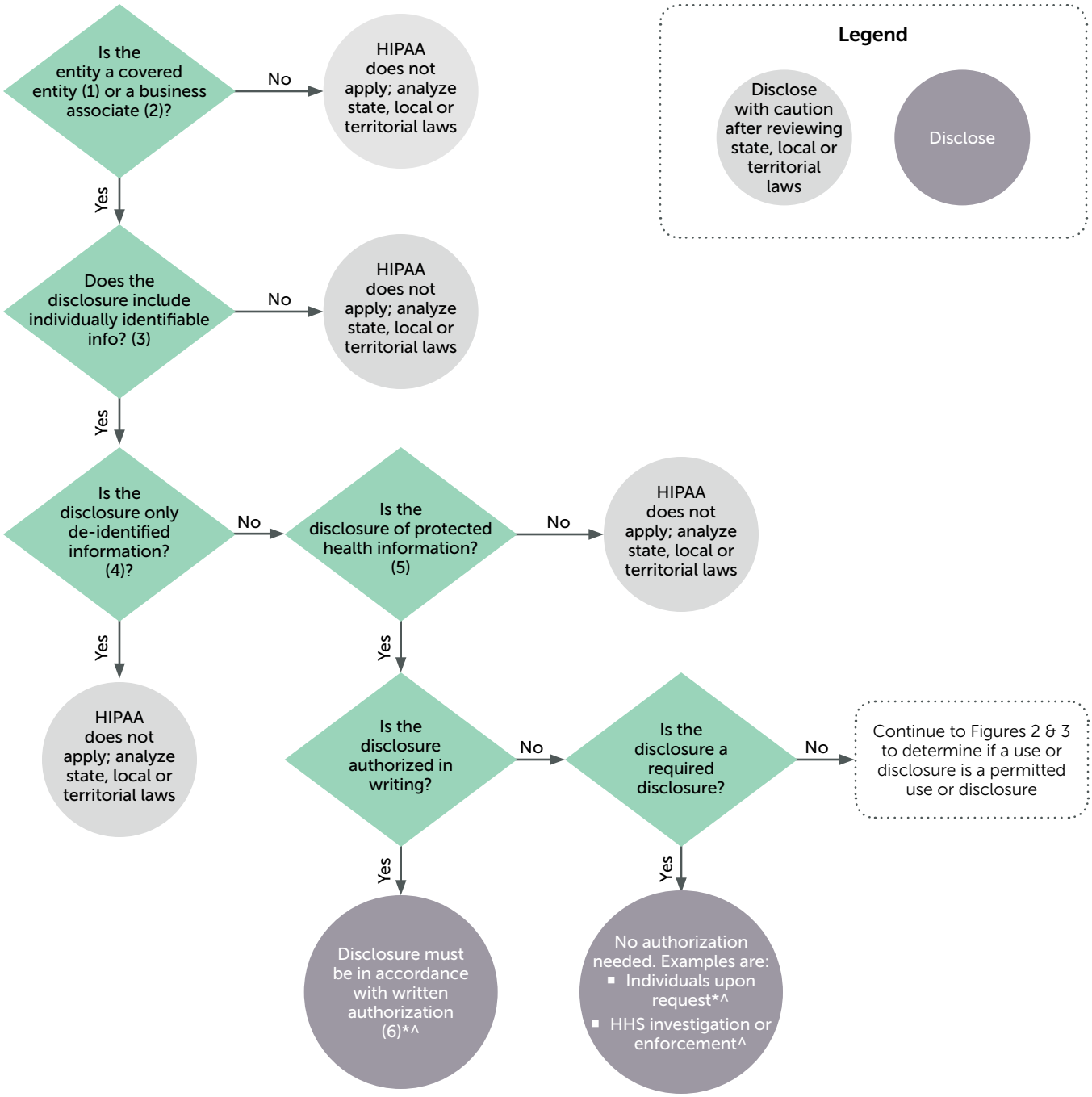


Figure 1. HIPAA authorized and required use and disclosure

***Minimum necessary.** When using, disclosing, or requesting PHI, a CE must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard applies to some, but not all, uses and disclosures. The minimum necessary standard does not apply to authorized or required disclosures.

^Accounting. Under HIPAA, individuals have a right to an accounting of the disclosures of their PHI by a CE or the CE's business associate. A CE that discloses information to an IIS is required to keep track of those disclosures. CEs (e.g., health care providers) are required to account for public health disclosures. An IIS that is a CE is required to keep an accounting of its disclosures, as required by the Privacy Rule. Authorized and required disclosures are not subject to the accounting requirement.

Table 2. Definitions of terms relating to HIPAA authorized and required disclosures

1	**Covered entity (CE)**	The Privacy Rule applies to health care providers, insurers, and clearinghouses that transmit standard electronic transactions (CEs or CE). The Privacy Rule does not exclude state agencies. If a state agency fits the definition of a CE under the Privacy Rule, the Privacy Rule applies to the state agency. However, many state agencies that house an IIS are not CEs because the agency does not provide, bill or receive payment for health care services (for example, if Medicaid is housed in a different state agency from the IIS). Even if the state agency housing the IIS is a CE, the state agency can choose to be a "hybrid entity" under the Privacy Rule. A hybrid entity is one that provides both covered functions and non-covered functions. The state agency can designate the areas that are covered functions and therefore CEs under the Privacy Rule, thereby excluding the remainder of the agency from the Privacy Rule. About forty-five percent of IIS consider the IIS to be part of a covered function (i.e., a CE) under the Privacy Rule.[37]
2	**Business associate (BA)**	A business associate (BA) is a person or entity that performs certain functions "on behalf of" a CE involving the use, disclosure or creation of PHI. The term BA excludes members of the CE workforce. It is important to note that the person or entity must be performing a function on behalf of the CE and not on behalf of itself. For example, an IIS is not, in general, a BA of a health care provider because the IIS is not providing a function or service on behalf of the health care provider. If an IIS is a CE, it must examine its relationship with any individual or entity that uses or accesses PHI in the IIS. To be a BA, the individual or entity must be providing one of the covered functions, activities or services for the IIS. Disclosures for treatment do not create a BA relationship; therefore, many disclosures of IIS data will not result in a BA relationship. However, if the IIS information is used for data analysis, billing, accreditation (accreditation organizations are specifically BAs), management, administrative, or legal purposes for or on behalf of the IIS, the data recipient will be a BA. In many cases, IIS application vendors, technology, and programmatic contractors are BAs of an IIS. A CE may not disclose PHI to a BA unless it obtains "satisfactory assurances" that the BA will safeguard the PHI. "Satisfactory assurances" usually means a business associate agreement (BAA). If both the CE and the BA are governmental agencies, the satisfactory assurances can be in a memorandum of understanding (MOU) or in applicable laws. Because of HITECH amendments to HIPAA, BAs are directly subject to HIPAA requirements. However, a BAA (or similar satisfactory assurances) is still required and may establish a separate contractual liability to the CE. See Table 3 for the definition of business associate agreement (BAA).
3	**Individually identifiable information**	"Individually identifiable health information" is information, including demographic data, that relates to: ■ The individual's past, present or future physical or mental health or condition, ■ The provision of health care to the individual, or ■ The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
4	**De-identified data**	De-identified data is not individually identifiable and is not covered by the Privacy Rule. De-identified data has a very specific definition under the Privacy Rule. Either a qualified statistician can certify that the data cannot be identified, or a list of eighteen identifiers must be removed from the data. Of particular relevance to uses of IIS information, the day/month of all dates must be removed from the data.
5	**Protected health information**	The Privacy Rule applies to protected health information (PHI). Protected health information is individually identifiable information held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral.

[37] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303.

6	**Written authorization**	A CE must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations, to a public health authority or otherwise permitted or required by the Privacy Rule. An authorization must be written in specific terms. It may allow use and disclosure of PHI by the CE seeking the authorization, or by a third party. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other information.

All other disclosures are permissive and unless there is a specific exception require a written authorization. However, two categories of permissive disclosures do require a form of consent, but not a written authorization.

1) A CE is permitted to disclose PHI under certain circumstances (provided the parent/individual has an opportunity to object), such as directory information, to relatives, friends and others who are assisting with health care and for notification in emergencies.

2) The second situation that does not require a written authorization is of particular importance to IIS. A CE can disclose proof of immunization to a school if the parent has requested the release (oral or written request) and the CE documents the request. Even if the IIS is a CE, disclosure to a school does not create a BA relationship between the IIS and the school.

Figure 2 below illustrates permissive disclosures under HIPAA with an opportunity to object or to schools upon request while Table 3 provides referenced definitions.

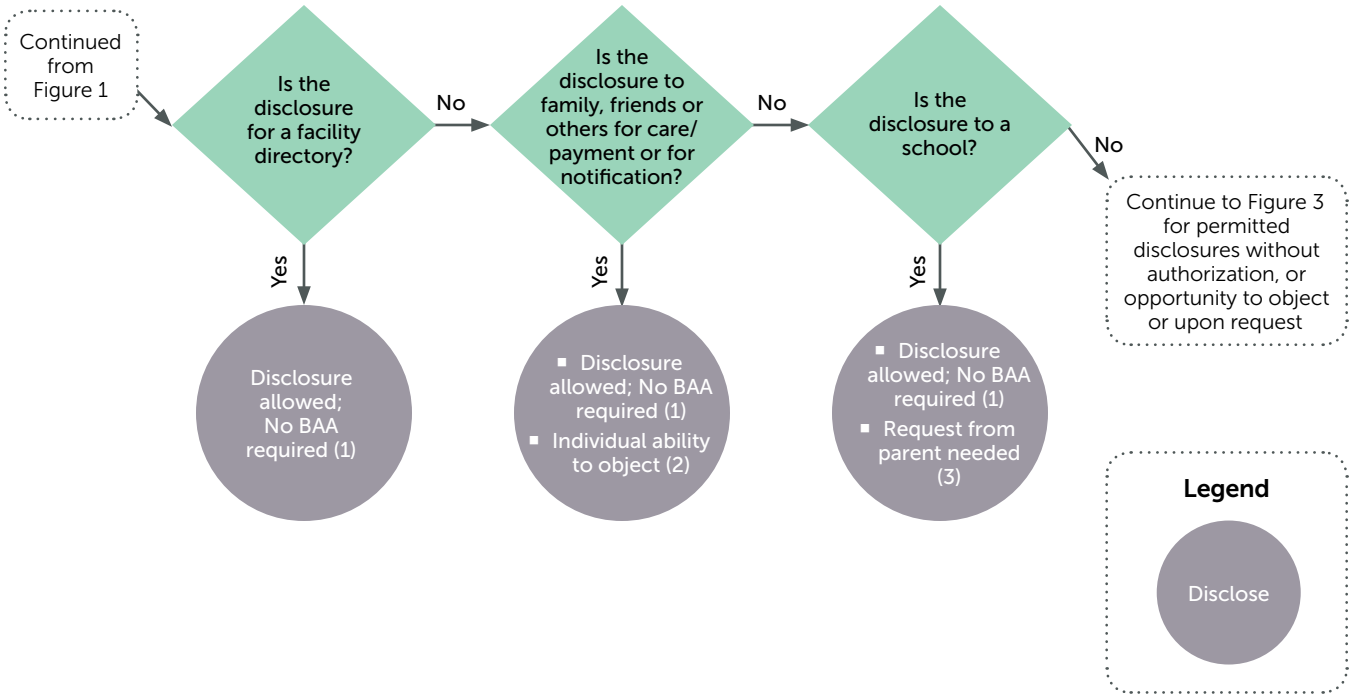


Figure 2. HIPAA disclosure permitted with opportunity to object or upon request

Table 3. Defined terms relating to HIPAA permitted disclosures with opportunity to object or upon request

1	**Business associate agreement (BAA)**	When a CE uses a contractor or other non-workforce member to perform BA services or activities, the Privacy Rule requires that the CE include satisfactory assurances for the safeguarding of the information in a business associate agreement (BAA), or similar arrangement. If a CE and its BA are both governmental entities, the protections can be included in a memorandum of understanding or in laws/regulations adopted by one of the governmental agencies. No BAA is required for disclosures permitted with authorization, opportunity to object or upon request to a school.
2	**Ability to object**	A CE is permitted, but not required, to use or disclose protected health information in certain circumstances in which the individual is informed in advance of the use or disclosure and has the opportunity to object, or in an emergency the CE determines that disclosure is in the best interest. The CE may orally inform the individual of and obtain the individual's oral agreement or objection to a permitted use or disclosure. In these circumstances, disclosure is permitted for limited protected health information.
3	**Informal request for disclosure to schools**	The CE must document a written or oral request for disclosure from the parent. Disclosure is limited to proof of immunization.

A CE may disclose PHI without authorization, opportunity to object or request in the circumstances illustrated in Figure 3. Table 4 below includes referenced definitions.

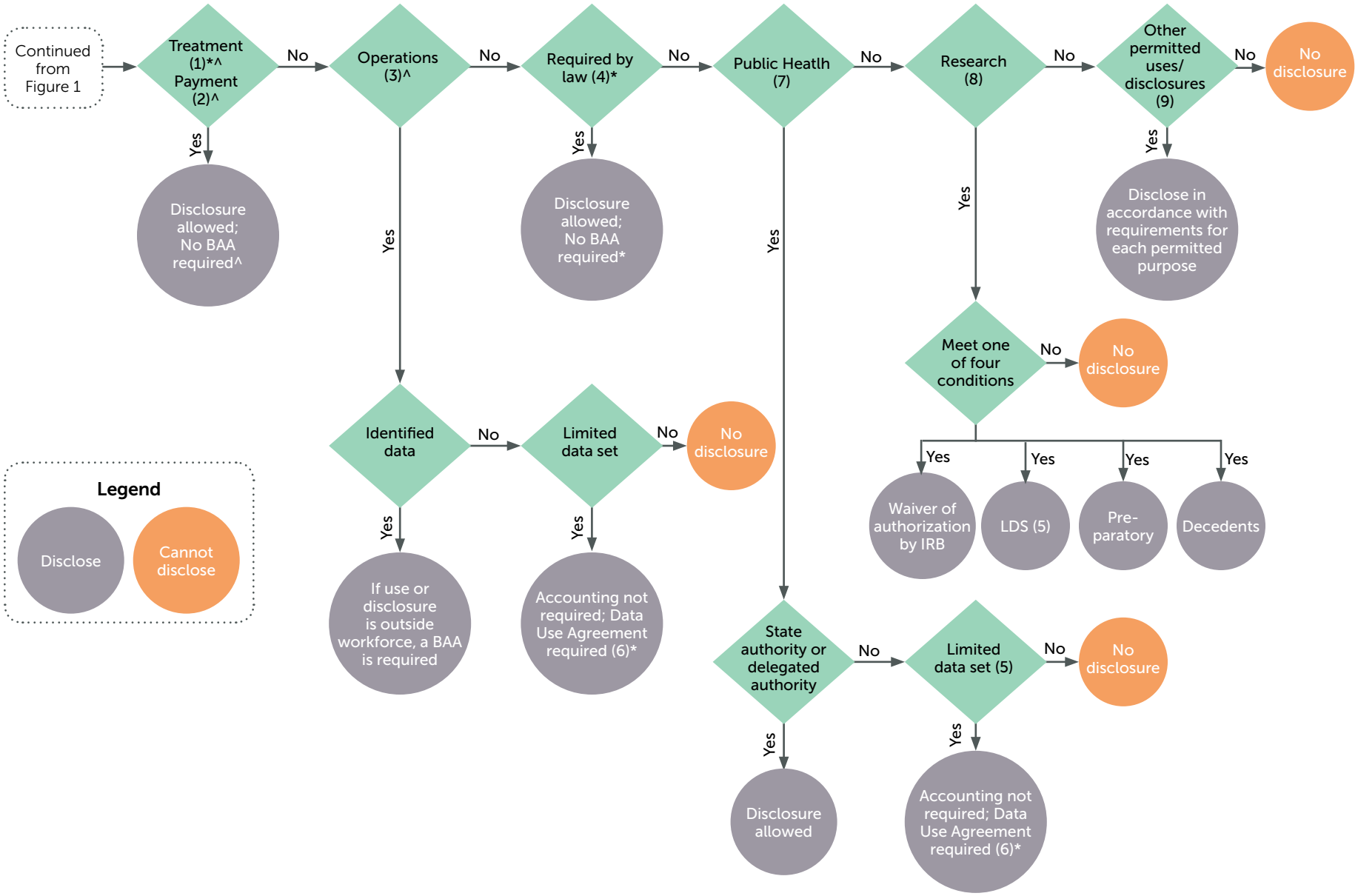


Figure 3. HIPAA permitted disclosures without authorization, opportunity to object or upon request

***Minimum necessary.** When using, disclosing, or requesting PHI, a CE must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard applies to some, but not all, uses and disclosures. The minimum necessary standard does not apply to disclosures for treatment or if as required by law; however, for disclosures required by law, the disclosure is limited to that required by the applicable law.

^Accounting. Under HIPAA, individuals have a right to an accounting of the disclosures of their PHI by a CE or the CE's BAs. A CE that discloses information to an IIS is required to keep track of those disclosures. CEs (e.g., health care providers) are required to account for public health disclosures. An IIS that is a CE is required to keep an accounting of its disclosures, as required by the Privacy Rule. The accounting requirement does not apply to disclosures for treatment, payment, healthcare operations or for a limited data set.

Table 4. Defined terms relating to HIPAA permitted disclosures without authorization, opportunity to object or upon request

1	**Treatment**	CEs may use or disclose PHI for treatment activities to another health care provider. Disclosure for treatment purposes does not make the recipient a BA, so no BAA is required for use or disclosure for treatment purposes. A CE is not required to account for treatment disclosures and the minimum necessary standard does not apply.
2	**Payment**	CEs may disclose PHI for payment purposes. Disclosure for payment purposes does not create a BA relationship. A CE is not required to account for payment disclosures.
3	**Operations**	CEs may disclose PHI for health care operations. If the disclosure is of individually identifiable information, most activities and functions that fall under health care operations trigger a BA relationship (if the disclosure is outside the CE's workforce) under HIPAA (for example, legal, data quality, accreditation, etc.) and a BAA is required. Alternatively, the disclosure can be of a limited data set, in which case the required data use agreement serves as a BAA. There is no accounting required for disclosures for health care operations under HIPAA.
4	**Required by law**	A CE can disclose PHI without an authorization if the disclosure is required by law. The minimum necessary standard does not apply; however, the amount of information disclosed is limited by the legal requirements. No BA relationship is created so a BAA is not required.
5	**Limited data set**	A limited data set is PHI from which 16 specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations and public health purposes provided the recipient enters into a data use agreement promising specified safeguards for the PHI within the limited data set. Accounting is not required for a limited data set. Compare a limited data set to de-identified data in which 18 direct identifiers must be removed. An important difference between a limited data set and de-identified data is that a limited data set can include a day/month in certain dates, while a de-identified data set cannot.
6	**Data use agreement**	A CE may use or disclose a limited data set only if the CE enters into a data use agreement in which the data recipient agrees it will only use or disclose the PHI for limited purposes. A data use agreement may be used in place of a BAA for a release of a limited data set for health care operations purposes. A data use agreement between the CE and the limited data set recipient must: ■ Establish the permitted uses and disclosures of such information ■ Establish who is permitted to use or receive the limited data set ■ Provide that the limited data set recipient will: ▪ Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law ▪ Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement ▪ Report to the CE any use or disclosure of the information not provided for by its data use agreement of which it becomes aware ▪ Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information ▪ Not identify the information or contact the individuals

7	**Public health**	A CE may disclose PHI without authorization to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions and to entities that have been delegated public health authority. Most data coming to an IIS is disclosed by a CE under the public health authority exception to HIPAA. IIS are considered to be public health authorities that are authorized by law to collect information to prevent and control disease. See guidance from CDC and HHS.[38] No BA relationship is created—the CE does not need a BAA from the IIS for the CE to release immunization information to the IIS. The minimum necessary standard does apply, but the CE can rely on the public health authority (the IIS) to specify the minimum amount of information needed for the public health purposes. The IIS should specify the minimum information required from the CE in its confidentiality policies and procedures and/or a local HL7 implementation guide. Release of information from one IIS to another IIS (interstate data exchange) would also be permitted without authorization under the Privacy Rule as a release to a public health authority; however, state, local and territorial laws may have additional requirements. The Partnership for Public Health Law and ASTHO are good resources for an overview of the legal issues surrounding interstate data sharing and a sample memorandum of understanding for IIS to IIS data sharing.[39]
8	**Research**	The Privacy Rule defines research as a systematic investigation including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a CE to use and disclose PHI for research purposes, without an individual's authorization, if the use or disclosure: (1) is approved by an Institutional Review Board or Privacy Board (IRB); (2) is solely to prepare a research protocol, the PHI is not removed from the CE, and is necessary for the research; or (3) is for research on the PHI of decedents. No BA relationship is created for research disclosures. The IRB approval or data use agreement provide limits on the information that can be released. A CE also may use or disclose, without an individuals' authorization, a limited data set of PHI for research purposes. IRB approval and accounting are not required. A data use agreement is required to disclose a limited data set.
9	**Other Permitted Uses/ Disclosures**	The Privacy Rule has several other exceptions to the requirement for an authorization that are less prevalent in the context of IIS. For example, a CE can release PHI to law enforcement, for health oversight, in abuse or neglect situations, and in judicial proceedings. Each of these exceptions is further defined in the Privacy Rule along with the requirements for disclosure in each circumstance.

[38] http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

[39] http://www.astho.org/Public-Policy/Public-Health-Law/Cross-Jurisdictional-Sharing-IIS-Data/, http://www.astho.org/Public-Policy/Public-Health-Law/IIS-MOU/

HIPAA Breach Notification Rule

The Breach Notification Rule requires CEs and BAs to notify individuals of unauthorized acquisition, access, use or disclosure under the Privacy Rule or the Security Rule (called a 'breach') of unsecured PHI. Impermissible use or disclosure of PHI is presumed to be a breach unless the CE can demonstrate a low probability that the PHI was compromised. The Rules gives four standards to determine if the PHI is compromised:

- Nature and extent of PHI involved
- Persons to whom disclosure made
- Whether the PHI was actually viewed or acquired
- Extent to which risk of breach was mitigated

The Breach Notification Rule contains an exception for secured PHI (HHS has provided guidance on technologies (such as encryption) and methodologies that render PHI secured). Guidance on secured PHI and the Security Rule will be addressed in a separate AIRA document.

FERPA Applied to IIS

Under FERPA, personally identifiable information contained in an education record cannot be disclosed without written consent of the parents or eligible student. The written and dated consent (which can be electronic) must specify the records to be released, the reasons for the release, and the parties to whom the information is to be released. Re-disclosures are not allowed unless the written consent also specifies the same items with respect to the re-disclosure.

A school can release de-identified education records if the school makes a reasonable determination that a student's identity is not personally identifiable. A school can release directory information (including the student's name; address; telephone listing; electronic mail address; date and place of birth; dates of attendance; and the most recent educational agency or institution attended) if it has given public notice of the disclosure and there is no objection.

A school may disclose personally identifiable, non-directory information from education records under a health or safety emergency exception only if the school determines, on a case-by-case basis, that a specific situation presents imminent danger or threat to students or other members of the community, or requires an immediate need for information in order to avert or diffuse serious threats to the safety or health of a student or other individuals. This exception is limited to the time period of the emergency and, in general, does not allow a blanket release of personally identifiable information from a student's education records to comply with general requirements under state, local and territorial laws.

There is no exception for the release of education records for routine public health purposes as in HIPAA. FERPA governs schools and not IIS. HIPAA governs IIS and not schools.

State, Local and Territorial Laws Applicable to IIS

HIPAA sets a floor for the protection of an individual's rights concerning certain health information and preempts less restrictive state (as state is defined in HIPAA) laws; however, it does not preempt more stringent laws. State, local and territorial laws that govern use and disclosure of IIS information IIS are varied and can include laws and regulations that authorize the operation of IIS and more general laws governing health care information and information held by public agencies. IIS should consult legal counsel or other appropriate local authorities concerning the application of state, local and territorial laws.

Chapter 4. IIS Confidentiality Policies and Practices

CDC developed IIS Functional Standards for 2013-2017 (Functional Standards) to lay a framework for the development of IIS through 2017 and will develop functional standards for years beyond 2017.40 In the Functional Standards CDC recognizes that information in IIS must be secure and confidential in programmatic goal 4, which requires IIS to: "[p]reserve the integrity, security, availability and privacy of all personally-identifiable health and demographic data in the IIS."[40] Functional Standard 4.1 requires each IIS to have "written confidentiality and privacy practices and policies based on applicable law or regulation that protect all individuals whose data are contained in the system."[40]

See Appendix G. Samples for examples of IIS confidentiality policies. IIS confidentiality practices and policies should be based on applicable laws and regulations (federal and state) and fair information practices. IIS that are CEs are required to comply with HIPAA, including requirements relating to notice of privacy practices and privacy policies and procedures. This Chapter provides practical considerations to assist IIS in developing confidentiality and privacy practices and policies. See Appendix A. Detailed Analysis of HIPAA and Appendix C. Fair Information Practices.

Several sections of this Chapter contain checklists. The individual checklists are combined into a single, searchable and more comprehensive document in Appendix G. Master Checklist for Confidentiality.

Guiding Principles

The guiding principles set forth in the CDC Confidentiality Chapter in 2000 (unpublished) are still applicable today. As in 2000, the confidentiality policy considerations in this document are designed to protect the privacy of IIS participants and the confidentiality of individually identifiable information contained in the IIS. The considerations for confidentiality policies in this document are based on the following principles that were stated in the CDC Confidentiality Chapter in 2000:

1. "The protection of privacy and the maintenance of confidentiality are essential to maintain the trust of the community, especially as use of IIS data increases."
2. "The confidentiality policies discussed in this [Chapter] are designed to balance the clinical and public health need for information and the privacy rights of the individual."
3. "The confidentiality policies in this [Chapter] are based on the principles of fair information practice, including the individual's right to know what information about him or her is in a record and how it is used, and to request amendments or corrections to the record."
4. "An IIS is a tool for monitoring and improving population-based health as well as the personal health of individuals regarding vaccine preventable diseases."
5. "The decision whether or not to participate in the registry and the decision whether or not to vaccinate are separate and distinct decisions."
6. "All IIS, including IIS that are part of integrated information systems, or that exchange information through a health information organization, must ensure that privacy is protected."

[40] http://www.cdc.gov/vaccines/programs/iis/func-stds.html

Topics to Cover in Confidentiality Policies

Even though the language of applicable laws may differ from IIS to IIS, IIS should consider addressing each of the following topics in its confidentiality policies.

General Provisions

- Confidentiality policies should be in written (electronic) form. CDC IIS 2013-2017 Functional Standard 4.1 requires that the confidentiality policies be in written format.[41]
- Confidentiality policies should be available to anyone who asks for them, for example, the confidentiality policies could be easily accessible through the IIS website.
- Confidentiality policies should be reviewed regularly (for example, annually) by legal counsel or other appropriate authority to ensure that they are consistent with applicable federal, state, local and territorial laws.
- Confidentiality policies should apply to everyone who has authorized use of information in the IIS, or authorized access to information in the IIS, including workforce, consultants, authorized users and business associates.
- Confidentiality policies should apply to all individually identifiable information in all formats including paper-based and electronic records.

Citation to Applicable Federal, State, Local and Territorial Laws

Each IIS must determine if it is subject to HIPAA. See HIPAA Applied to IIS above and Appendix A. Detailed Analysis of HIPAA. In addition, each IIS must examine its state, local and territorial laws to determine which apply to it.

Checklist for authority to collect information

✔ Examine state, local and territorial laws to determine authority to operate the IIS for each age group included in the IIS

State, local and territorial laws authorize the operation of IIS and may be specific to the IIS or may be general public health laws. In 2013, 68% of IIS collected immunization information for children under specific state statutes, 19% under general public health authority, 11% under immunization information sharing laws, and 2% under laws allowing sharing of general health information.[42] Fewer states had specific statutory authority to collect immunization information with respect to adults and therefore relied more on general public health or data sharing authority.[42] More specific rules or regulations may implement the statutory authority. In addition to providing the authority to collect information, the statutes and any rules or regulations will also provide the basis for a statement concerning the purpose for the collection of the data, for example, preventing or controlling disease. Recitation of the statutory authority (and implementing regulations) to collect information and the purpose of the collection is important to assure health care providers submitting information to the IIS that they can rely on the public health authority exception to HIPAA. See Chapter 3. HIPAA Applied to IIS above and Appendix A. Detailed Analysis of HIPAA.

Notice

Notification can inform parents/individuals that information about the individual will be included in an IIS and of the potential uses and disclosures of the information. Notice is an important aspect of the principles of fair information practices. See Appendix C. Fair Information Practices. CEs under HIPAA are required to comply with Privacy Rule requirements concerning the contents and timing for providing a notice of privacy practices. See Appendix A. Detailed Analysis of HIPAA.

In addition to the requirements for notice of privacy practices in HIPAA (if applicable) entities that disclose information to an IIS, and IIS, must comply with applicable state, local and territorial laws. State, local and territorial laws may be silent with respect to notice requirements, or may have specific requirements about the information that must be

[41] http://www.cdc.gov/vaccines/programs/iis/func-stds.html

[42] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303.

included in the notice, who gives the notice and when and how it is given. For example, state, local and territorial laws may require that the IIS or a health care provider, or both, give notice directly to the parent/individual at the time of first treatment. State, local and territorial laws may require notice that information is to be included in the IIS be given to one age group (for example, adults) and not to a different age group (for example, parents of children). On the other hand, state, local and territorial laws may not require notice to parents/individuals that information will be included in the IIS. Not requiring notice may be more prevalent in states that mandate reporting of immunizations to the IIS. In 2013, almost 60% of jurisdictions operating an IIS mandated at least one type of provider to report immunizations to the IIS.[43]

Checklist for notice (e.g., that information will be included in an IIS and/or notice of privacy practices under HIPAA)

- ✔ Determine if a notice is required, for example, HIPAA applies or state, local and territorial laws requires a notice
- ✔ If notice is required, determine:
  - Who must provide notice
  - Notice contents
  - Notice timing
  - Form of notice (e.g., written)

Content of Notice

A CE must follow HIPAA (if applicable) and state, local and territorial laws concerning the content and delivery of a notice. State, local and territorial laws may be silent concerning the content of a notice. HIPAA provides that a notice of privacy practices must describe in plain language:

- How the CE may use and disclose protected health information about an individual.
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the CE.
- The CE's legal duties with respect to the information, including a statement that the CE is required by law to maintain the privacy of protected health information.
- Whom individuals can contact for further information about the CE's privacy policies.

IIS and entities disclosing information to the IIS should also consider including information about how to exercise choice about inclusion of information in the IIS (See Choice, below) if the state, local and territorial laws provides choice.

Providing the Notice

Under HIPAA, a CE must make its notice of privacy practices available to any person who asks for it, and prominently post and make available its notice on any website it maintains that provides information about its customer services or benefits. Covered direct treatment providers must also provide the notice of privacy practices to the individual no later than the date of first service delivery and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice.

State, local and territorial laws differ concerning requirements on how notice of inclusion of information in an IIS must be given (if a notice is required at all).

For example, state, local and territorial laws may require that notice of inclusion of information in an IIS be:

- Posted by health care providers,
- Available on the IIS or health care provider website, or
- Mailed to parents of newborns.

[43] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303.

Choice (Consent)

Once a parent/individual has been notified that their information will be included in the IIS or even if the parent/individual is not notified that their information is included in the IIS, he or she may have the ability to choose whether or not to participate in the registry. HIPAA does not require an authorization for a CE to release information to an IIS. (See Chapter 3. HIPAA Applied to IIS above and Appendix A. Detailed Analysis of HIPAA). However, many states have specific laws governing consent for participation in the IIS. If state, local and territorial laws are more restrictive than HIPAA, IIS and health care providers must comply with the state, local and territorial laws.

State, local and territorial laws governing the ability to choose whether to participate in an IIS will require one of several types of consent. The general types of consent are: consent is implied (assumed) and the parent/individual has a right to choose to exclude or not to be included in the IIS (known as a right to "opt-out"), no consent is required (with or without a right to opt-out), and explicit consent in oral or written form (known as "opt-in"). A variety of data sources populates IIS. One data source for demographic information (and Hep B, in some states) is information on births from vital records or birthing hospitals. Requirements for consent to populate an IIS with vital records vary. The consent type also may differ based on age, for example, one type of consent for children and a different type of consent for adults. There may also be differences in consent requirements based on the type of provider administering an immunization. For example, some states have different consent requirements for pharmacists than for other health care providers.

Checklist for consent requirements

- ✔ If HIPAA applies, determine if proposed disclosure is permitted without authorization
  - To an IIS (HIPAA public health exception)
  - To an individual (HIPAA exception)
  - To health care provider (HIPAA exception for treatment purposes)
  - To researcher (HIPAA exception with limitations)
  - Other
- ✔ Examine state, local and territorial laws for consent requirements for each age group included in the IIS (childhood, adolescent, adult)
  - Examine following types of laws
    - Laws authorizing operation of an IIS
    - Specific laws/policies governing vital records
    - Laws defining scope of practice laws for the provider type
      - Traditional (for example, pediatricians)
      - Non-traditional (for example, pharmacist)
  - Determine the type of consent (if any) required for each age group in the IIS
    - No consent required
    - Implicit consent with opt-out
    - No consent; with opt-out
    - No consent; no opt-out
    - Explicit consent
  - Determine requirements for consent and withdrawal (if allowed)
    - Oral or written consent
    - How to withdraw consent
    - Type of documentation
    - Who retains documentation
- ✔ Determine effect of opt-out on information in the IIS
  - Purge
  - Limit access

The following table shows the percentage of IIS by consent type, data source and age group (as of 2012).[44]

Table 5. Types of consent to include information in an IIS

Type of Consent	Information from vital records	Information from health care providers	
		For children	For adults
Explicit (either oral or written)	11%	8%	16%
Implied consent; with ability to opt-out	45%	68%	66%
No consent; with ability to opt-out	11%	4%	1%
No consent required; no ability to opt-out	33%	23%	16%

Effect of Opt-out on Information in the IIS

If a parent/individual opts-out of the IIS after information has been included in the IIS, there are varying requirements in state, local and territorial laws about how to treat the information concerning that individual. In 2012, all data were retained and access was limited or prohibited in 70% of IIS that permitted opt-out, all data were removed in 7% and limited demographic information was retained in 6%.[44] Removal of data can result in the information being re-entered into the IIS multiple times with the need to remove the information again. In an IIS that retains limited demographic information, information can be kept out of the IIS; however, if a parent/individual decides to opt-in after an opt-out, all immunization information must be re-entered into the IIS.

Permitted Use/Disclosure

IIS confidentiality policies should indicate the individuals and entities permitted to use or disclose information in the IIS and any limitations on those uses and disclosures. Each IIS should review its authorizing state, local and territorial laws to determine the individuals and entities permitted to access information in the IIS and any requirements or limitations on use and disclosure. In addition to state, local and territorial laws, IIS that are CEs under HIPAA should determine the requirements under HIPAA for any proposed use and access (disclosure) of PHI, keeping in mind that if state, local or territorial laws are more restrictive than HIPAA concerning use and disclosure of IIS information the state, local or territorial laws will control.

General Considerations

State, local and territorial laws may have a list of persons/entities permitted to access IIS information. Examples of the persons/entities that might be included in such a list are: the individual, health care practitioners (which could be limited to those who administer vaccines), health care clinics, local public health, schools and child care, parents, managed care organizations, state Medicaid agency, Veterans Administration, Indian Health Services, long term care, health exchange organizations, researchers, other state agencies, and other IIS (interstate data exchange). If there is not a specific list in an IIS authorizing statute, the IIS must reference other state, local and territorial laws to determine persons and entities permitted to use and access IIS information.

Authority to access information in the IIS is not sufficient for an IIS to provide access. Every person or entity that accesses information in the IIS must be authorized by the IIS to obtain access. To be authorized to access IIS information the person or entity should sign a user agreement or site agreement and agree to comply with applicable federal, state, local and territorial laws and the IIS confidentiality policies. See Site Agreement/User Agreement section below.

Checklist for permitted use/disclosure

- ✔ Determine if HIPAA applies/has applicable exception to authorization
- ✔ Examine state, local and territorial laws to determine
  - Permitted persons/entities for use/disclosure of IIS information by age group included in the IIS
  - Permitted purposes for use/disclosure of IIS information by age group in the IIS and by type of person/entity
- ✔ Examples of permitted persons/entities for use/disclosure
  - To the individual
  - Research
  - Schools
  - Health care providers

[44] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303.

Release of information from one IIS to another IIS (one type of interstate data exchange) is, in general, permitted without authorization under the Privacy Rule as a release to a public health authority. However, each IIS should examine applicable laws and policies in its jurisdiction to determine if it is permitted to release data outside its borders to another IIS and any requirements for documentation. The Partnership for Public Health Law and ASTHO prepared an overview of the legal issues surrounding interstate data sharing and a sample memorandum of understanding for interstate data sharing.[45]

In addition to permitted persons and entities, state, local and territorial laws will provide permitted purposes for which IIS information can be accessed and disclosed. State, local and territorial laws could broadly permit use and disclosure of IIS information for any public health purpose, or state, local and territorial laws could have a list of permitted purposes for the release of immunization information, for example:

- To the parent/individual who is the subject of the record
- To the extent necessary for the treatment, control, investigation, and prevention of vaccine-preventable diseases (which could be further limited to the licensed health care practitioner treating the person who is the subject of an immunization record),
- To a health maintenance organization for compliance
- To a school in which such person is enrolled for school entry law purposes
- To others, for purposes specified by state, local and territorial laws

In addition to permission under state, local and territorial laws for persons and entities to use and access information in the IIS for specified purposes, IIS that are CEs must comply with HIPAA. Disclosures permitted under HIPAA are described in Chapter 3. HIPAA Applied to IIS above and in Appendix A. Detailed Analysis of HIPAA.

Minimum Necessary Standard

Most health care providers that submit information to an IIS are governed by HIPAA. Under HIPAA, disclosures of PHI must be the minimum amount of information necessary to accomplish the purpose of the permitted disclosure. The submitting health care provider can rely on the IIS to establish the minimum necessary for the purposes of the IIS. The IIS can establish the minimum necessary (e.g., data elements) in its confidentiality policies or in other policies, for example, its HL7 local implementation guide.

With respect to use and disclosure of information after it is in the IIS, a separate analysis is necessary. State, local and territorial laws may establish parameters that limit the information that can be released. If the IIS is a CE, it must establish policies and procedures concerning the minimum amount of information required for each use and disclosure of PHI. The minimum necessary standard does not apply to disclosures to a health care provider for treatment purposes but does apply to uses by a CE's workforce. For uses of protected health information, policies and procedures should identify the persons or classes of persons within the IIS workforce who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. Some public health agencies may have policies applicable across the workforce of the entire agency, and policies related to role-based access may also be located in security policies. Case-by-case review of each use is not required. For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required. For non-routine disclosures and requests, CEs must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly.

The IIS could consider a matrix of permitted uses and disclosures, the type of access and the amount of information that can be used/disclosed. Each IIS will need to examine its authorizing laws and regulations to determine authorized uses/disclosures. Examples follow in Table 6 and Table 7. Each IIS will have different authorized uses/disclosures and varying levels of access.

[45] http://www.astho.org/Public-Policy/Public-Health-Law/Cross-Jurisdictional-Sharing-IIS-Data/, http://www.astho.org/Public-Policy/Public-Health-Law/IIS-MOU/

Table 6. Example of workforce matrix

Job Title	IIS Module with PHI	Limitations
Program Manager	All	Need-to-know
School Coordinator	School	Need-to-know; school module only
Web designer	No access to PHI	Not Applicable

Table 7. Example of non-workforce matrix

User Type	View Demographics and Immunization information	Purpose	Add/Edit Demographics and Immunization information	Reports	Ordering and Inventory
Immunization provider (public and private)	Yes	Treatment	Yes	Yes	Yes (limited)
School	Yes (with documented request from parent)	Proof of required immunization	No	No	No
Researcher	No access to database; results of ad hoc queries are furnished to researcher	Epidemiological studies, as provided under applicable IRB approval	No	No	No

Research

If an IIS is a CE, HIPAA contains specific requirements relating to disclosures for research purposes. Many state, local and territorial laws also contain specific requirements for disclosures for research purposes. IIS should consider addressing requirements for research requests in their confidentiality policies. Topics to consider are: no publication without approval, no-redisclosure, confidentiality statements by each user, IRB that must give approval, requirements for agreements to protect confidentiality of data, limited data set and data use agreement under HIPAA, and MOU requirements if the requesting entity is another governmental agency.

Data Retention and Disposal

An IIS that is a CE must maintain its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented for six years.

Various state, local and territorial laws may govern the length of time that immunization information must be maintained or in some cases, must be destroyed. Specific IIS authorizing state, local and territorial laws may have time limits for maintaining immunization information which may depend on the age of the child or individual who is the subject of the information. Broader public data retention state, local and territorial laws may govern the time that state information will be maintained, with the time ranging from a few years to forever.

Checklist for data retention and disposal

- ✔ Determine if HIPAA applies
  - General six-year retention period
- ✔ Examine state, local and territorial laws to determine
  - What to retain
  - Retention time

Rights of Individual to Access, Inspect and Amend

If an IIS is a CE, the parent/individual has the right to access, inspect and request an amendment of information in a designated data set, except in limited circumstances. CEs may impose reasonable, cost-based fees for the costs. The Privacy Rule specifies processes for requesting and responding to a request for amendment. A CE must amend PHI in its designated record set upon receipt of notice to amend from another CE.

For IIS that are not governed by HIPAA, and to determine if state, local and territorial laws is more restrictive than HIPAA, the IIS should examine state, local and territorial laws for rights of an individual to access, inspect and amend IIS information. Applicable provisions may be contained in authorizing IIS laws or in more broadly applicable state, local and territorial laws.

Checklist for rights of individuals to access, inspect and amend

- ✔ Determine if HIPAA applies
  - Individuals have rights to access, inspect and request amendment of their information in a designated record set
- ✔ Examine state, local and territorial laws to determine individual's rights to access, inspect and amend

Disclosure Accounting

Under HIPAA, individuals have a right to an accounting of the disclosures of their PHI by a CE or the CE's BAs. A CE that discloses information to an IIS is required to keep track of those disclosures. An IIS that is a CE is required to keep an accounting of its disclosures as required by the Privacy Rule. Disclosures for treatment purposes are not subject to the accounting requirements.

Point of Contact at IIS and at Authorized Entity

The IIS and each authorized entity must designate a privacy officer to be the point of contact for all issues relating to the IIS confidentiality policies.

Breach Notification

Under HIPAA if there is a breach of unsecured PHI, a CE must provide notification of the breach to affected individuals, the Secretary of the U.S. Department of Health and Human Services, and, in certain circumstances, to the media. In addition, BAs must notify CEs if a breach occurs at or by the BA. With respect to a breach at or by a BA, while the CE is ultimately responsible for ensuring that individuals are notified, the CE may delegate the responsibility of providing individual notices to the BA. CEs and BAs should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the BA performs on behalf of the CE and which entity has the relationship with the individual.

Checklist for breach notification

- ✔ If HIPAA applies, notice to
  - affected individuals
  - the Secretary of HHS
  - sometimes to media
  - the CE if the breach is at a business associate
- ✔ Determine if state, local and territorial laws contains breach notification requirements

Under HIPAA, a CE should not be responsible for notification of a breach by an entity (other than a BA) to whom the CE made a permitted disclosure.

However, in addition to HIPAA requirements, more and more states are adopting requirements concerning breach notifications in statutes authorizing IIS and more broadly applicable laws. State, local and territorial laws that are more stringent than HIPAA will control.

Sanctions

HIPAA provides for civil penalties for violations, but they are not enforceable through private actions. Individuals can file complaints about HIPAA violations with OCR.

Many state, local and territorial laws also impose sanctions for violation of confidentiality requirements.

Checklist for sanctions

- ✔ Determine if HIPAA applies
  - Civil and criminal penalties
- ✔ Examine state, local and territorial laws to determine sanctions for violations of state, local and territorial laws

Site Agreement/User Agreement

IIS ensure the confidentiality of IIS information by requiring that each individual provided access to IIS information agrees to abide by the IIS confidentiality policies and applicable federal, state, local and territorial laws. IIS can enter into a confidentiality agreement with each individual user (user agreement) or with an entity that in turn requires anyone it provides IIS access to abide by the IIS confidentiality policies and applicable federal, state, local and territorial laws (site agreement), or by a combination of site agreements and user agreements.

Many IIS began operations with each user logging into the IIS through a user interface and very little data coming into the IIS electronically. The IIS managed access through passwords issued to individuals and user agreements.

In recent years, IIS receive and return more data through electronic data transfers from electronic health records with less direct access to the IIS by individuals. IIS must increasingly ensure the confidentiality of the information in the IIS through agreements with the health care entities responsible for the information in an electronic health record (site agreement).

State, local and territorial laws and policies may require an IIS to use site agreements, user agreements or both. Advantages and disadvantages of user agreements and site agreements can also guide an IIS as it determines the best approach to ensure the confidentiality of information.

With user agreements, the IIS maintains control over authentication (passwords) with increased control over access of IIS information. However, because of the large number of individual users for any IIS, management of the authentication is burdensome. Managing individual access controls is also less feasible with electronic submission and query of IIS information.

With site agreements, the IIS must rely on the signing authority to enforce confidentiality at the individual level. Site agreements may be the most feasible solution with electronic submission and query of IIS.

Considerations for provisions to include in user agreements:

- Appropriate authorities will review the user agreement regularly (e.g., at least annually) to ensure continuing compliance with federal, state, local and territorial laws
- The individual agrees to:
  - Comply with the IIS confidentiality policies and federal, state, local or territorial laws with respect to IIS information
  - Only access information that the individual has a need to know to perform her/his duties
  - Not share her/his IIS password with anyone
  - Notify the IIS immediately about any unauthorized use/disclosure of IIS information

Considerations for provisions to include in site agreements:

- Appropriate authorities will review the site agreement regularly (e.g., at least annually) to ensure continuing compliance with federal, state, local and territorial laws
- The site agrees to:
  - Enforce the IIS confidentiality policies
  - Issue passwords to individuals and to enforce prohibitions on sharing passwords
  - Inform the IIS within a reasonable amount of time after any authorized IIS user becomes ineligible to be an IIS authorized user
  - Keep an audit trail of all persons who access/use information received from the IIS
  - Notify the IIS immediately about any unauthorized use/disclosure of IIS information

Chapter 5. Scenarios

The following scenarios are intended to provide general guidance in how to analyze various situations concerning use and disclosure of IIS information. The scenarios are not legal advice and are not a substitute for legal counsel. Each IIS should consult its own legal counsel to determine how federal, state, local and territorial laws affect use and disclosure of IIS information. Since federal laws provide a floor for protection of health information, the scenarios examine the impact of these federal laws on confidentiality of information in IIS. The scenarios do not address state, local and territorial laws. The facts in any real scenario will differ and may result in a different result under federal laws. Readers are encouraged to contact appropriate individuals within their own agency who are responsible for interpretation and implementation of federal, state, local and territorial laws governing privacy and confidentiality.

Table 8. Scenarios

Scenario		Facts	Analysis	Results
1.	Information submitted to the IIS	An OB/GYN clinic is reluctant to send immunization information to the IIS because of concerns that HIPAA prohibits it to share immunization information without authorization from the patient.	Review state, local or territorial laws to determine that OB/GYN clinics are authorized to report to the IIS. For example, in a state that authorizes the IIS to collect data for children (and not adults) an OB/GYN clinic may not be authorized to send immunization information to the IIS. See Figure 3. HIPAA permitted disclosures without authorization, opportunity to object or upon request and Table 4, Reference 7, Public Health.	If the OB/GYN clinic is authorized (but not mandated) to send immunization information to the IIS under state, local or territorial laws, it may, but is not required to, send the immunization information to the IIS without authorization from the patient under HIPAA.
2.	Information disclosed by the IIS to others	A public health professor requests immunization information from the IIS to examine the rate of flu vaccine uptake over the prior three flu seasons.	Determine whether the IIS is governed by HIPAA. Determine if data is de-identified and not subject to HIPAA. Determine if the request is considered to be research. Determine if IRB approval has been obtained. Determine if data requested can be satisfied with a limited data set. See Figure 3. HIPAA permitted disclosures without authorization, opportunity to object or upon request and Table 4, Reference 8, Research.	If HIPAA applies, de-identified data can be released with no restrictions from HIPAA. Data for research purposes can be released without authorization in limited circumstances in accordance with an IRB approval or as a limited data set with a data use agreement. State, local or territorial laws may be more restrictive than HIPAA.

Scenario		Facts	Analysis	Results
3.	Health Information Exchange Organization (HIO)	User in provider organization office accesses IIS information through an electronic health record. Electronic health record accesses IIS through an HIO.	Examine the relationship of each entity to each other entity in the data flow to ensure that each actor maintains the confidentiality of IIS information.	User has an (employment) agreement with the provider in which the user agrees to maintain confidentiality of IIS information. The provider organization has an agreement with its EHR vendor in which the vendor agrees to maintain the confidentiality of the IIS information. The provider organization has an agreement with the HIO in which the HIO agrees to maintain the confidentiality of the IIS information. The IIS, through the Department of Health, has an agreement with the HIO in which the HIO agrees to maintain the confidentiality of the IIS information.*
4.	Electronic Health Record (EHR)	User in provider organization office accesses IIS information through an EHR (or the information from the IIS is incorporated in the EHR).	Examine the relationship of each entity to each other entity in the data flow to ensure that each actor maintains the confidentiality of IIS information.	User has an (employment) agreement with the provider in which the user agrees to maintain confidentiality of IIS information. The provider organization has a BA agreement with its EHR vendor, in which the vendor agrees to maintain confidentiality of the IIS information. The provider organization has a site agreement with the IIS in which it agrees to maintain the confidentiality of IIS information through enforcement of its confidentiality agreements with employees and others who access IIS information.

*The issues involved in examining HIOs in the context of submitting data to and accessing data from an IIS are complex and beyond the scope of this document. An HIO may itself be a CE under HIPAA. In addition, each step in the data flow must be analyzed separately to determine the impact of federal, state, local and territorial laws. Each submission/access of information through an HIO must be analyzed individually to determine if the HIO is a BA of the IIS, a BA of the entity submitting/accessing the information through the HIO, or both. Considerations include: 1) is the HIO an official state entity, 2) is submission/access through the HIO mandated by state, local and territorial laws, and 3) is the HIO a mere conduit (like an internet provider), or does it provide transmission or other services or functions that allow it access to PHI on a routine basis.

Conclusions

IIS are confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area. IIS are established and operated by states, municipalities, territories and the District of Columbia under applicable state, local and territorial laws.

The privacy of individuals whose information is contained in the IIS and the confidentiality of information disclosed to and by IIS are integral parts of IIS development and use. Often overlapping federal, state, local and territorial laws protect the confidentiality of information in IIS, but also recognize that health data can and should be shared appropriately to support individual and population health care.

This document is intended to provide the IIS community with considerations for confidentiality procedures and policies to meet legal requirements for protecting the privacy of individuals and maintain the confidentiality of information in an IIS. The information contained in this document is not legal advice nor should it substitute for legal counsel. Readers are encouraged to contact appropriate individuals within their own agency who are responsible for interpretation and implementation of federal, state, local and territorial laws governing privacy and confidentiality.

Appendix A. Detailed Analysis of HIPAA

Much of this Appendix is from the United States Health and Human Services (HHS) website[46] on the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. HIPAA contains provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. See Appendix D. Glossary for definitions of terms used in this Appendix.

The HHS website provides a short history of the rules adopted by HHS to implement HIPAA (as they relate to privacy and confidentiality of IIS information), as follows:[46]

- HHS published the Privacy Rule in December 2000 (modified in August 2002). The Privacy Rule sets national standards to ensure the privacy of individuals and the confidentiality of protected health information (PHI) by three types of CEs: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.
- HHS published the Security Rule in February 2003. The Security Rule sets national standards for security aspects the confidentiality, integrity, and availability of electronic PHI.
- HHS enacted the Omnibus Final Rule in January 2013 to implement some provisions of the Health Information Technology for Clinical and Economic Health Act (HITECH Act),[47] including additional privacy and security protections, and to finalize the Breach Notification Rule.
- The Combined Regulation Text (as of March 2013) contains all the HIPAA rules in one (unofficial) document. The Code of Federal Regulations (C.F.R.) at 45 C.F.R. §§ Part 160, Part 162, and Part 164 contains the official HIPAA rules.

This paper examines the impact of the Privacy Rule[48] on IIS, as modified by the Omnibus Rule, and certain aspects of the Breach Notification Rule. A separate AIRA paper will examine the impact on IIS of the Security Rule[49] and the security aspects of the Breach Notification Rule.[50]

Privacy Rule

General

The Privacy Rule establishes a set of national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of PHI by CEs and as well as standards for individuals' rights with respect to their health information. The Office for Civil Rights ("OCR") in the U.S. Department of Health and Human Services (HHS) is responsible for implementing (including education and guidance) and enforcing the Privacy Rule.

Who is Governed by the Privacy Rule

The Privacy Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA ("covered entity" or "CE"). See 45 C.F.R. § 160.103.

- Health Plans. Individual and group plans that provide or pay the cost of medical care are CEs. Health plans include health, dental, vision, and prescription drug

[46] http://www.hhs.gov/hipaa/for-professionals/index.html

[47] Health Information Technology for Clinical and Economic Health Act ("HITECH"), February 17, 2009, 111 Public Law.

[48] *Standards for Privacy of Individually Identifiable Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.160_07.html, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.164_07.html

[49] *Security Standards for the Protection of Electronic Protected Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Part 160 and Subparts A and C of Part 164, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.160_07.html, http://www.access.gpo.gov/nara/C.F.R./waisidx_07/45C.F.R.164_07.html

[50] *Notification in the Case of Breach of Unsecured Protected Health Information*, Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations, Subpart D of Part 164, https://www.gpo.gov/fdsys/pkg/C.F.R.-2011-title45-vol1/pdf/C.F.R.-2011-title45-vol1-sec164-400.pdf

insurers, health maintenance organizations, Medicare, Medicaid, Medicare supplement, and long-term care insurers. See 45 C.F.R. § 160.103.

- Health Care Providers. Every health care provider who electronically transmits health information in connection with certain transactions is a CE. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under HIPAA. Health care providers include all providers of medical or health services (e.g., hospitals, physicians, dentists and other practitioners) and any other person or organization that furnishes, bills, or is paid for health care. See 45 C.F.R. § 160.103.
- Health Care Clearinghouses. Health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard format or data content. See 45 C.F.R. § 160.103.

CEs in the IIS community

An entity that submits immunization data to an IIS may or may not be a CE. Immunization providers, hospitals and health insurers are, in general, CEs under HIPAA. IIS may or may not be CE, depending on whether the agency housing the IIS furnishes, bills, or receives payment for health care services. Some public health agencies do not furnish, bill or receive payment for health care services and are not subject to HIPAA.

A CE that is a single legal entity and that conducts both covered and non-covered functions can elect to be a "hybrid entity." See 45 C.F.R. §§ 164.103 and 164.105. The activities that make a person or organization a CE are its "covered functions." See 45 C.F.R. § 164.103. If a CE designates in writing its operations that perform covered functions as one or more "health care components" then most of the Privacy Rule applies only to the health care components. If a CE does not make a designation as a hybrid entity, then all its functions are subject to the Privacy Rule. Approximately 45% of IIS are considered to be CE under HIPAA.[51]

Business Associate

Business Associate Defined. In general, a business associate (BA) is a person or organization that performs certain functions or activities on behalf of, or provides certain services to, a CE that involve the use or disclosure of individually identifiable health information. BA functions or activities on behalf of a CE include claims processing, data analysis, and billing (See 45 C.F.R. § 160.103). BA services to a CE are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Persons or organizations are not BAs if the functions or services do not involve the use or disclosure of PHI, or access to PHI would be incidental. A CE can be the BA of another CE. See 45 C.F.R. § 160.103.

The HITECH Act made BAs directly responsible for many provisions of HIPAA and made clear that a subcontractor of a business associate who creates, receives, maintains, or transmits PHI on behalf of the business associate is also a business associate under HIPAA. A BA's privacy obligations must be documented in a business associate agreement, or similar assurance. A BA must enter into a business associate agreement with its BA subcontractors that satisfies HIPAA's detailed requirements for a business associate agreement. See 45 C.F.R. § 164.502(e)(1)(ii) and Business Associate Agreement (BAA) below.

Figure 4 is a visual representation of the analysis to determine if a person/entity is a BA in the situations most common to IIS operations.

[51] Immunization Information Systems: A Decade of Progress in Law and Policy, Martin, Daniel W. MSPH; Lowery, N. Elaine JD, MSPH; Brand, Bill MPH; Gold, Rebecca JD; Horlick, Gail MSW, JD, Journal of Public Health Management & Practice: May/June 2015 - Volume 21 - Issue 3 - p 296–303

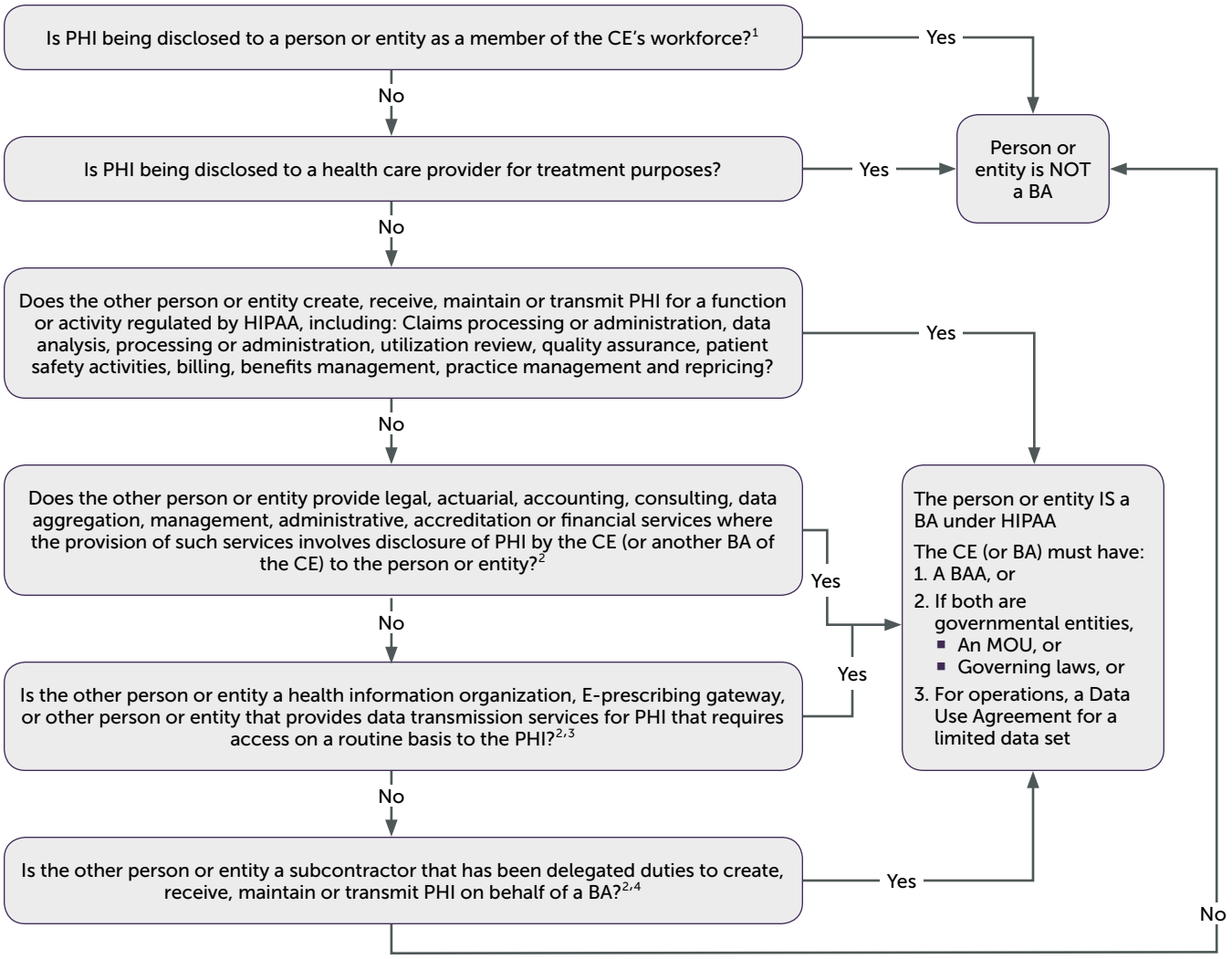


Figure 4. Business Associate Decision Tree (in the context of IIS)

[1] Workforce includes persons who are under the direct control of a CE or a BA. See 45 C.F.R. § 160.103.

[2] See 45 C.F.R. § 160.103 for the complete definition of business associate.

[3] Health maintenance organization is not defined in the Privacy Rule to allow the industry to develop. See FR p. 5571, Vol. 78, No. 17, Jan 25, 2013. Transient conduits (such as an internet service provider) that provide mere transmission service are not included. A health information organization with a master patient index is not a mere conduit. See FR pp. 5571-72, Vol. 78, No. 17, Jan 25, 2013.

[4] For example, a shredding company for PHI is a subcontractor. See Federal Register 5573, Vol. 78, No. 17, Jan 25, 2013.

Business Associate Agreement (BAA). When a CE uses a BA to provide functions or services on behalf of the CE, the Privacy Rule requires that the CE include satisfactory assurances for the safeguarding of PHI used by or disclosed to the BA in a BA agreement, or similar arrangement. If a CE and its BA are both governmental entities, the assurances can be included in a memorandum of understanding or in laws/regulations adopted by one of the agencies. See 45 C.F.R. §§ 164.502(e), 164.504(e). A CE may not authorize its BA to make any use or disclosure of PHI that would violate HIPAA. A BA may use or disclose protected health information only as permitted or required by its BA contract or similar assurances, or as required by law. A BA that subcontracts with another BA must enter into a BAA with its BA subcontractors that satisfy HIPAA's detailed requirements for such agreements.

A BAA must:

- Establish the permitted and required uses and disclosures of PHI by the BA. In general, the contract may not authorize the BA to use or further disclose the information in a manner that the CE could not do.
- Provide that the BA will, among other things:
  - Not use or further disclose the information other than as permitted or required by the contract or as required by law
  - Ensure the security of the PHI
  - Report any breaches
  - Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same provisions that apply to the BA
  - Make available PHI to the individual and HHS
  - Make available PHI for amendments
  - Make available the information required to provide an accounting of disclosures in accordance with the Privacy Rule
  - At termination of the contract, if feasible, return or destroy all PHI
  - Be subject to termination by the CE if the BA breaches the BAA. See 45 C.F.R. § 164.504(e); 45 C.F.R. § 164.308 (b).

What Information is Protected

PHI. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral. This information is protected health information (PHI). See 45 C.F.R. § 160.103.

Individually identifiable health information is information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual,
- The past, present, or future payment for the provision of health care to the individual, and

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. See 45 C.F.R. § 160.103. See the list of identifiers that must be removed to de-identify data under De-Identified Health Information.

The Privacy Rule excludes from PHI records subject to FERPA (the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g).

De-Identified Health Information. De-identified health information is not subject to HIPAA. See 45 C.F.R. §§ 164.502(d)(2) and 164.514(a) and (b). De-identified health information must not identify or provide a reasonable basis to identify an individual. There are two ways to de-identify information: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers., See 45 C.F.R. § 164.514(b)

The following identifiers of the individual, relatives, employers, or household members of the individual must be removed to meet the "safe harbor" method of de-identification (See 45 C.F.R. § 164.514(b):

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code under certain circumstances
- All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) showing ages over 89
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes if certain conditions are met

Uses and Disclosures

General Principles

A CE may use or disclose PHI, as authorized by the individual who is the subject of the information in writing (See 45 C.F.R. § 164.502(a)), and as permitted or required by the Privacy Rule.

Authorized Disclosures

A CE must obtain the individual's written authorization for any use or disclosure of PHI that is not permitted or required by the Privacy Rule. It may allow use and disclosure of PHI by the CE obtaining the authorization, or by a third party. Authorizations must be written in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other information. See 45 C.F.R. § 164.532.

Required Disclosures

A CE must disclose PHI in only two situations: (a) to individuals (or their personal representatives) when they request access to, or an accounting of disclosures of, their PHI; and (b) to HHS when it is undertaking an investigation or enforcement. See 45 C.F.R. § 164.502(a)(2). Release to state or local public health is not required by federal law, but may be required by state, local and territorial laws. See Required by Law below.

Permitted Uses and Disclosures

Opportunity to object. A CE is permitted, but not required, to use or disclose protected health information, in a limited number of circumstances in which the individual is informed in advance of the use or disclosure and has the opportunity to object. The CE may orally inform the individual of and obtain the individual's oral agreement or objection to a permitted use or disclosure. See 45 C.F.R. § 164.510. Examples are:

- Facility directory
- To a relative, friend or other person involved in the individual's health care
- Notification
- Disaster relief

No opportunity to object. In addition to situations in which HIPPA allows use/disclosure of information in which there is an opportunity to object, a CE is permitted, but not required, to use and disclose PHI without authorization: 1) for treatment, payment and health care operations; 2) incident to an otherwise permitted use and disclosure; 3) for public interest and benefit activities; and 4) in a limited data set for the purposes of research, public health or health care operations. See 45 C.F.R. § 164.502(a)(1). A CE may use its own judgement in deciding which of these permitted uses and disclosures to make.

Treatment, Payment, Health Care Operations. A CE may use and disclose PHI for its own treatment, payment, and health care operations activities. See 45 C.F.R. § 164.506(c). A CE also may disclose PHI for the treatment and payment activities of another health care provider under certain circumstances. Obtaining "consent" (written permission from individuals to use and disclose their PHI for treatment, payment, and health care operations) is optional under the Privacy Rule for all CEs. See 45 C.F.R. § 164.506(b).

- Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation and referral. See 45 C.F.R. § 164.501.
- Payment includes activities of a health care provider and health plans relating to payment or reimbursement for health care services. See 45 C.F.R. § 164.501.
- Health care operations include a CE's administrative, financial, and quality improvement activities. Health care operations include the following: 1) conducting quality assessment and improvement activities, including outcome evaluation and development of clinical guidelines, so long as the activity is not research ; 2) population-based activities relating to improving health or reducing health care costs, protocol development, and case management and care coordination; 3) accreditation, certification, and licensing, and 4) management and administrative activities, including de-identifying PHI and creating a limited data set. 45 C.F.R. § 164.501.

Incidental Use and Disclosure. The Privacy Rule does not require elimination of every risk of an incidental use or disclosure of PHI. A use or disclosure of PHI that is incident to an otherwise permitted use or disclosure is permitted as long as the CE has adopted reasonable safeguards, and the information being shared is limited to the minimum necessary. See 45 C.F.R. § 164.502(a)(1)(iii).

Public Interest. The Privacy Rule permits use and disclosure of PHI, without authorization, for specified purposes related to benefit to the public. See 45 C.F.R. § 164.512. Specific conditions or limitations apply to each purpose. The Privacy Rule defines state as any of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands and Guam. Local and territorial IIS should consult their own attorney to determine the interaction of local and territorial laws with HIPAA. Examples are:

- ***Required by Law.*** A CE may use and disclose PHI without individual authorization as required by law (including by statute, regulation, or court orders). See 45 C.F.R. § 164.512(a).
- ***Public Health Activities.*** The HIPAA exception that permits most disclosures to an IIS is the public health authority exception. CEs may disclose PHI to public health authorities authorized by law to collect or receive the information for preventing or controlling disease, injury, or disability, and to entities that have been delegated public health authority. See 45 C.F.R. § 164.512 (b) (1) (i). The definition of public health authority includes IIS authorized to operate under state, local and territorial laws. See 45 C.F.R. § 164.512 (b) (1) (i).
- ***Schools.*** A CE can release PHI to a school about an individual who is a student or prospective student of the school, if: (A) the information is limited to proof of immunization; (B) the school is required by state law to have proof of immunization; and (C) the CE obtains and documents the agreement (which can be oral or written) to the disclosure from the parent/individual. See 45 C.F.R. § 164.512(b)(1)(vi). Comments on the final rule state that the written authorization requirement was removed from release to schools to help facilitate disclosure of proof of immunization to school, but a parent is required to contact a child's health care provider (or IIS if it is a CE) to request that proof of immunization be sent to the child's school. The Privacy Rule requires "active agreement from the appropriate individual, and a health care provider may not disclose immunization records to a school under this provision without such agreement". FR p. 5617, vol. 78, No 17, Jan 25, 2013. "The agreement must be an affirmative assent or request by a parent to the covered entity, which may be oral and over the phone, to allow the disclosure of the immunization records. A mere request by a school to a health care provider for the immunization records of a student is not sufficient to permit disclosure under this provision." FR pp. 5617-5618, vol. 78, No 17, Jan 25, 2013. The comments also clarify that the "Privacy Rule at § 164.512(a) permits a covered entity to use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. As such, the Privacy Rule does not prohibit immunization disclosures that are mandated by State law, nor does it require authorization for such disclosures. However, with regard to State laws that permit but do not require covered entities to disclose immunization records to schools, this does not meet the requirements of the provisions at § 164.512(a), and disclosures of immunization records are subject to the Privacy Rule agreement and documentation requirements [described in this paragraph]." FR pp. 5618, vol. 78, No 17, Jan 25, 2013.
- ***Communicable Disease.*** A CE may disclose PHI to individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law. See 45 C.F.R. § 164.512.
- ***Victims of Abuse, Neglect or Domestic Violence.*** In certain circumstances, a CE may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence. See 45 C.F.R. § 164.512(a), (c).
- ***Health Oversight Activities.*** A CE may disclose PHI to health oversight agencies. See 45 C.F.R. § 164.512(a), (c).
- ***Judicial and Administrative Proceedings.*** A CE may disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. PHI may also be disclosed in response to a subpoena in certain instances. See 45 C.F.R. § 164.512(e).
- ***Law Enforcement Purposes.*** A CE may disclose PHI to law enforcement officials for law enforcement purposes in some circumstances. See 45 C.F.R. § 164.512(f).
- ***Research.*** The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501. The Privacy Rule permits a CE to use and disclose PHI for research purposes, without an individual's authorization, if the use and disclosure is approved by an Institutional Review Board or Privacy Board. See 45 C.F.R. § 164.512(i). A CE also may use or disclose, without an individuals' authorization, a limited data set of PHI for research purposes (see Limited Data Set below). See 45 C.F.R. § 164.514(e).

Limited Data Set

A limited data set may be used and disclosed for research, health care operations, and public health purposes, if the recipient enters into a data use agreement for the PHI within the limited data set. A CE is not required to provide an accounting when it uses PHI to create a limited data set. Limited data sets are excepted from the accounting requirement. See 45 C.F.R. § 164.528(a) (1)(viii).

- *Identifiers.* A limited data set is PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. See 45 C.F.R. § 164.514(e). A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual (See 45 C.F.R. § 164.514(e)(2)):
  - Names
  - Postal address information, other than town or city, State and zip code
  - Telephone numbers
  - Fax numbers
  - Electronic mail addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers including license plate numbers
  - Device identifiers and serial numbers
  - Web Universal Resource Locators (URLs)
  - Internet Protocol (IP) address numbers
  - Biometric identifiers, including finger and voice prints
  - Full face photographic images and any comparable images
- *Data Use Agreement.* A CE may use or disclose a limited data set only if the CE enters into a data use agreement in which the data recipient agrees it will only use or disclose the PHI for limited purposes. A data use agreement must:
  - Establish the permitted uses and disclosures of such information. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate HIPAA if done by the CE
  - Establish who is permitted to use or receive the limited data set
  - Provide that the limited data set recipient will
    - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - Report to the CE any use or disclosure of the information not provided for by its data use agreement
  - Ensure that any agents to whom it provides the limited data set agree to the same restrictions and
  - Not identify the information or contact the individuals

Minimum Necessary Standard

A CE must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed. See 45 C.F.R. §§ 164.502(b) and 164.514 (d). A CE must develop and implement policies and procedures to limit uses and disclosures to the minimum necessary. See 45 C.F.R. §§ 164.502(b) and 164.514 (d).

The minimum necessary requirement does not apply to: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with HIPAA. See 45 C.F.R. §§ 164.502(b) and 164.514 (d).

Access and Uses. A CE must have policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to PHI to carry out their duties, the categories of PHI to which access is needed, and any conditions under which they need the information to do their jobs. See 45 C.F.R. §§ 164.502(b) and 164.514 (d).

Disclosures and Requests for Disclosures. A CE must have policies and procedures for routine, recurring disclosures, or requests for disclosures, that limits the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, a CEs must develop criteria designed to limit disclosures to the minimum necessary and review each of these requests individually in accordance with the established criteria. See 45 C.F.R. §§ 164.502(b) and 164.514 (d).

Reasonable Reliance. If another CE or a BA of a CE makes a request for PHI, a CE may rely on the request as complying with the minimum necessary standard. Similarly, a CE may rely upon requests as being the minimum necessary PHI from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the CE's BA, or (c) a researcher who provides the documentation required by the Privacy Rule for research. The request must be reasonable under the circumstances and the CE is not required to rely on the request as being the minimum necessary. See 45 C.F.R. §§ 164.502(b) and 164.514 (d).

Notice and Other Individual Rights

Notice of Privacy Practices.

The Privacy Rule provides that an individual has a right to adequate notice of how a CE may use and disclose PHI about the individual, the individual's rights and the CE's obligations with respect to the PHI. Most CEs must develop and provide individuals with this notice of their privacy practices. See 45 C.F.R. §§ 164.520(a) and (b).

- *Content of the Notice.* CEs are required to provide a notice in plain language that describes:
  - How the CE may use and disclose protected health information about an individual
  - The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the CE
  - The CE's legal duties with respect to the information, including a statement that the CE is required by law to maintain the privacy of protected health information
  - Whom individuals can contact for further information about the CE's privacy policies
- *Providing the Notice.* A CE must make its notice available to any person who asks for it and prominently post and make available its notice on any website it maintains that provides information about its customer services or benefits. A direct treatment CE must also provide the notice to the individual no later than the date of first service delivery. See 45 C.F.R. §§ 164.520(a) and (b).
- *Acknowledgement of Notice Receipt.* A direct treatment CE must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice, except in an emergency treatment situation. See 45 C.F.R. §§ 164.520(a) and (b). The Privacy Rule does not require any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement.
- *Multiple Notices.* Any CE, including a hybrid entity, may choose to develop more than one notice, such as when an entity performs different types of covered functions and there are variations in its privacy practices among these covered functions.

State, local and territorial laws may require additional requirements for the content, delivery and acknowledgement of privacy/confidentiality practices and of notice of inclusion of information in an IIS.

Access. Individuals have the right to review and obtain a copy of their PHI in a CE's designated record set. See 45 C.F.R. § 164.524. The designated record set is that group of records maintained by or for a CE that is used, in whole or part, to make decisions about individuals. See 45 C.F.R. § 164.501. A CE may impose reasonable, cost-based fees for the costs.

Amendment. The Rule gives individuals the right to request that a CE amend their PHI in a designated record set. See 45 C.F.R. § 164.526. If a CE accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it and to persons that the CE knows might rely on the information to the individual's detriment. A CE may deny an individual's request for amendment if: (a) the information is not available for access under the Privacy Rule; (b) the CE did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer

available); (c) the CE determines that the information is accurate and complete; or (d) the information is not in a designated record set. If the request is denied, the CE must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. A CE must amend PHI in its designated record set upon receipt of notice to amend from another CE. See 45 C.F.R. § 164.526.

Disclosure Accounting. Individuals have a right to an accounting of the disclosures of their PHI by a CE or the CE's BAs. See 45 C.F.R. § 164.528. The maximum disclosure accounting period is the six years immediately preceding the accounting request.

The Privacy Rule does not require accounting for disclosures in certain situations, including: (a) for treatment, payment, or health care operations; (b) to the individual; (c) pursuant to an authorization; (d) of a limited data set; or (e) incident to otherwise permitted or required uses or disclosures.

Restriction Request. Individuals have the right to request that a CE restrict use or disclosure of PHI for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. See 45 C.F.R. § 164.522(a). A CE is under no obligation to agree to requests for restrictions. A CE that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Confidential Communications Requirements. Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the CE typically employs. See 45 C.F.R. § 164.522(b). For example, through a designated address or phone number or in a closed envelope rather than a post card.

Administrative Requirements

The Privacy Rule allows a CE to implement policies and procedures in a manner that is appropriate for the particular CE, taking into consideration the CE's size and resources.

- *Privacy Policies and Procedures.* A CE must have written privacy policies and procedures that are consistent with the Privacy Rule. See 45 C.F.R. § 164.530(i). Policies and procedures that address the Privacy Rule may cover all of a state agency, a portion of a state agency or be limited to only the IIS.
- *Privacy Personnel.* A CE must designate a privacy official responsible for its privacy policies and procedures, and a contact responsible for receiving complaints and providing individuals information about the CE's privacy practices. See 45 C.F.R. § 164.530(a).
- *Workforce Training and Management.* A CE must train all workforce members on its privacy policies and procedures. See 45 C.F.R. § 164.530(b). A CE must use appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule. See 45 C.F.R. § 164.530(e).
- *Data Safeguards.* A CE must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. See 45 C.F.R. § 164.530(c).
- *Complaints.* A CE must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. See 45 C.F.R. § 164.530(d). The CE must explain those procedures in its notice of privacy practices. See 45 C.F.R. § 164.520(b) (1) (vi).
- *Documentation and Record Retention.* A CE must maintain certain documentation for six years. Documentation that must be retained includes privacy policies and procedures, notices of privacy practices, and disposition of complaints. See 45 C.F.R. § 164.530(j).

Other Provisions

Personal Representatives and Minors

The Privacy Rule requires a CE to treat a personal representative the same as the individual with respect to uses and disclosures of PHI and the individual's rights under the Rule. See 45 C.F.R. § 164.502(g). A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule has an exception in cases of abuse, neglect or endangerment. In most cases, parents are the personal representatives for their minor children and can exercise individual rights, such as access to the medical record, on behalf of their minor children. HIPAA references state laws to determine if a parent is considered the personal representative of a minor child and to determine the rights of parents to access and control the PHI of their minor children. See 45 C.F.R. § 164.502(g).

State, Local and Territorial Laws

In general, state laws that are contrary to the Privacy Rule are preempted by the Privacy Rule. The Privacy Rule defines state as any of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands and Guam. Local and territorial IIS should consult their own attorney to determine if local and territorial laws are preempted by HIPAA. See 45 C.F.R. § 160.103 and § 160.201-203. However, the Privacy Rule does not preempt state laws that (1) provide greater rights with respect to PHI, or (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention.

Enforcement and Penalties for Noncompliance

Compliance. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for implementing and enforcing the Privacy Rule and may conduct complaint investigations and compliance reviews.

Civil Money Penalties. OCR may impose a penalty on a CE for violations of the Privacy Rule. Penalties range from $100 per violation to $50,000 per violation with a cap of $1.5 million in a calendar year. See 45 C.F.R. § 160.404.

Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $250,000 and up to 10 years of imprisonment. The Department of Justice is responsible for criminal penalties.

Emergency. HIPAA does not contain a specific exception for emergencies. HIPAA exceptions that could be used during an emergency include disclosures for treatment, to locate family members and to address imminent danger.

Breach Notification Rule

The HIPAA Breach Notification Rule requires HIPAA CEs and their BAs to provide notification following a breach of unsecured PHI. See 45 C.F.R. §§ 164.400-414. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. Breach notification is covered in this document because of its applicability to the confidentiality of IIS information. More detail on the security aspects of the breach notification rule will be addressed in a separate AIRA document dealing with the security of IIS information.

Definition of Breach

As stated above, a breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the CE or BA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors (See 45 C.F.R. §§ 164.402 (2)):

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

There are three exceptions to the definition of breach. See 45 C.F.R. § 164.402.

- Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority. The information cannot be further used or disclosed in a manner not permitted by the Privacy Rule
- Inadvertent disclosure of PHI by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the CE or BA. The information cannot be further used or disclosed in a manner not permitted by the Privacy Rule
- If the CE or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information

Unsecured PHI

CEs and BAs must provide notice only if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons using a technology or methodology specified by the Secretary in guidance. See 45 C.F.R. § 164.402.

Breach Notification Requirements

Following a breach of unsecured PHI, CEs must provide notification of the breach to affected individuals, the Secretary of HHS, and, in certain circumstances, to the media. In addition, BAs must notify CEs if a breach occurs at or by the BA. 45 C.F.R. §§ 164.406-410.

Individual Notice

CEs must notify affected individuals following the discovery of a breach of unsecured PHI.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the CE is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the CE (or BA, as applicable). 45 C.F.R. § 164.405.

With respect to a breach at or by a BA, while the CE is ultimately responsible for ensuring individuals are notified, the CE may delegate the responsibility of providing individual notices to the BA.

Media Notice

CEs that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. The media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice. 45 C.F.R. § 164.406.

Notice to the Secretary of HHS

In addition to notifying affected individuals and the media (where appropriate), CEs must notify the Secretary of HHS of breaches of unsecured PHI. If a breach affects 500 or more individuals, CEs must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the CE may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered. 45 C.F.R. § 164.408.

Notification by a BA

If a breach of unsecured PHI occurs at or by a BA, the BA must notify the CE following the discovery of the breach. A BA must provide notice to the CE without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the BA should provide the CE with the identification of each individual affected by the breach as well as any other available information required to be provided by the CE in its notification to affected individuals. 45 C.F.R. § 164.410.

Other Requirements

CEs and BAs are required to prove that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. 45 C.F.R. § 164.414.

CEs must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Appendix B. Detailed Analysis of FERPA

Much of the information in this Appendix is from the U.S. Department of Education website for guidance on the Family Educational Rights and Privacy Act of 1974 (FERPA).[52]

Introduction

FERPA is a Federal law that protects the privacy of student education records and creates rights with respect to those records for parents and eligible students (students over 18 years of age or who attend school beyond high school). The law applies to all educational agencies and institutions (elementary, secondary or post-secondary) that receive funds under any program administered by the Department of Education ("Department"). Private schools at the elementary and secondary school levels generally do not receive funds from the Department and are not subject to FERPA. It is important to keep in mind that FERPA governs what schools can do with information in education records. FERPA does NOT govern IIS or health care providers and does not limit what IIS or health care providers can or cannot disclose to schools. It is also important to note, however, that HIPAA applies to most health care providers and almost half of IIS. HIPAA allows CE to disclose PHI to schools if a parent/individual has requested the CE to make the disclosure.

Education Records: Included

Education records mean those records that are directly related to a student, and maintained by an educational agency or institution or by a party acting for the agency or institution. See 1232g (a) (4) (A); 34 C.F.R. § 99.3 A K-12 student's health records, including immunization records, maintained by an educational agency or institution subject to FERPA, including records maintained by a school nurse, would generally be "education records" subject to FERPA because they are 1) directly related to a student; 2) maintained by an educational agency or institution, or a party acting for the agency or institution; and 3) not excluded from the definition as treatment or sole possession records, or on some other basis. See 20 U.S.C. §1232g (a) (4)(a). Therefore, student immunization records that are maintained by an educational agency or institution subject to FERPA that directly relate to a student or students are considered education records under FERPA and are not subject to the HIPAA Privacy Rule.

Education Records: Excluded

School-based health clinics. If an outside party provides health care services directly to students and is not employed by, under contract to, or otherwise acting on behalf of the school, for example, a public health nurse who is not also a school nurse or otherwise acting on behalf of the school.

University student health centers. Medical treatment records for students who are 18 years or older or are attending postsecondary education are not education records if they are made, maintained, and used only in connection with treatment of the student and disclosed only to professionals providing the treatment. See 20 U.S.C. § 1232g (a) (4) (A).

General Rule: No Disclosure without Written Consent

Personally identifiable information contained in an education record cannot be disclosed without written consent of the parents/eligible student. See 20 U.S.C. §1232g (b) (1); C.F.R. § 99.30. FERPA regulations define personally identifiable information to include (See 34 C.F.R. § 99.3):

- The student's name
- The name of the student's parent or other family member
- The address of the student or student's family
- A personal identifier, such as the student's social security number or student number
- A list of personal characteristics that would make the student's identity easily traceable
- Other information that would make the student's identity easily traceable

[52] (20 U.S.C. § 1232g; HHS regulations at 34 C.F.R. § Part 99) http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

The written and dated consent (which can be electronic) must specify the records to be released, the reasons for the release, and the parties or class of parties to whom the information is to be released. See 20 U.S.C. §1232g (B) (2); 34 C.F.R. § 99.31 Re-disclosures are not allowed unless the written consent also specifies the same items with respect to the re-disclosure. See 34 C.F.R. § 99.33 (a) (1). An educational institution can release immunization information to an IIS in accordance with a consent that meets FERPA requirements. The consent should address whether information released to an IIS will be used/disclosed to any person or entity other than the educational institution (i.e., re-disclosed).

Disclosures Permitted without Written Consent

De-identified Records. Education records can be released after the removal of all personally identifiable information if the school has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. See 34 C.F.R. § 99.31 (b) (1).

Directory Information. Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. See 34 C.F.R. § 99.3. Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; date and place of birth; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; and the most recent educational agency or institution attended. See 34 C.F.R. § 99.3. Directory information does not include a student's social security number, or unique personal identifier. See 34 C.F.R. § 99.3.

An educational agency or institution may disclose directory information if it has given public notice to parents of students in attendance of:

(1) The types of personally identifiable information that the agency or institution has designated as directory information;

(2) A parent's right to refuse to let the agency or institution designate any or all of those types of information about the student as directory information; and

(3) The period of time within which a parent or eligible student has to notify the agency or institution in writing that he or she does not want any or all of those types of information about the student designated as directory information. See 34 C.F.R. § 99.37 (a).

Health and Safety Emergency. An educational agency or institution may disclose personally identifiable information from an education record to appropriate parties, including parents of an eligible student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals. An educational agency or institution may take into account the totality of the circumstances pertaining to a threat to the health or safety of a student or other individuals. If the educational agency or institution determines that there is an articulable and significant threat to the health or safety of a student or other individuals, it may disclose information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. See 34 C.F.R. § 99.36.

To release personally identifiable information from an education record under the health or safety emergency exception the agency or institution must determine "on a case-by-case basis, that a specific situation presents imminent danger or threat to students or other members of the community, or requires an immediate need for information in order to avert or diffuse serious threats to the safety or health of a student or other individuals. Any release must be narrowly tailored considering the immediacy and magnitude of the emergency and must be made only to parties who can address the specific emergency in question. This exception is temporally limited to the period of the emergency and generally does not allow a blanket release of personally identifiable information from a student's education records to comply with general requirements under state, local and territorial laws. Certainly an outbreak of diseases such as measles, rubella, mumps, and polio not only pose threat of permanent disability or death for the individual, but have historically presented themselves as epidemic in nature.

Thus, disclosure of personally identifiable information from students' education records to State health officials for such reasons would generally be permitted under FERPA's health or safety emergency provisions."[53]

Annual Notice

Schools are required to give annual notice to parents/eligible students about their rights under FERPA, including the right to inspect and amend education records and the right to consent to disclosures of PHI unless the disclosure is otherwise permitted under FERPA. See 34 C.F.R. § 99.7

Recordkeeping

FERPA establishes a recordkeeping requirement for educational agencies and institutions. See 34 C.F.R. § 99.32. An educational agency or institution is required to maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student for as long as the records are maintained. The record of disclosure is required to include the parties who requested/obtained the information and their reason to request/obtain the information. See 34 C.F.R. § 99.32.

[53] Letter to Alabama Department of Education Regarding Disclosure of Immunization Records, dated February 25, 2004, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/alhippaa.html

Appendix C. Fair Information Practices

Several national and international organizations have developed privacy frameworks to use as tools to help think about discussions about privacy. One set of privacy principles used internationally was developed by the Organization for Economic Co-operation and Development (OECD) in 1980 and revised in 2013.[54] In the United States, the Secretary of the Department of Health, Education and Welfare (HEW) created a Committee on Automated Personal Data Systems. In its 1973 report, the committee recommended adoption of five basic principles:

- "There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data".[55]

There are many versions of fair information practices.[56] A version developed by the Office of the National Coordinator of Health Information Technology, U.S. Department of Health and Human Services is found in the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information released in 2008, and states:[57]

- **Individual Access:** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
- **Correction:** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.
- **Openness and Transparency:** There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.
- **Individual Choice:** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.
- **Collection, Use, and Disclosure Limitation:** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
- **Data Quality and Integrity:** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
- **Safeguards:** Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- **Accountability:** These principles should be implemented and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

[54] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[55] http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm

[56] http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[57] http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

Appendix D. Glossary

Many of the definitions below are based on defined terms in HIPAA and FERPA. Please refer to HIPAA and FERPA for the official definitions.

Accounting, under HIPAA, refers to documentation of disclosures of PHI by a CE or the CE's BAs.

Authorization, under HIPPA, is an individual's consent to a use or disclosure of PHI that meets certain requirements under HIPAA.

Authorized users are those individuals or organizations permitted to use information in the IIS or that the IIS is permitted to disclose information to under state, local and territorial laws and IIS policies.

Business Associate (BA), under HIPAA, means a person or organization that performs certain functions or activities on behalf of, or provides certain services to, a CE that involve the use or disclosure of protected health information.

Business Associate Agreement (BAA), under HIPAA, means a CE's contract or other written arrangement with its BA, which must contain specified elements.

Confidentiality is the treatment of information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure.

Confidentiality policy is a written policy applicable to the information in the IIS that sets forth policies and procedures to protect an individual's privacy and the confidentiality of information in the IIS in accordance with applicable federal, state, local and territorial laws.

CE (covered entity), under HIPAA, means health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.

Data use agreement (DUA), under HIPAA, means an agreement between a CE and a limited data set recipient in which the data recipient agrees it will only use or disclose the PHI for limited purposes.

De-identified information neither identifies nor provides a reasonable basis to identify an individual. Under HIPAA, there are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of 18 specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the CE has no actual knowledge that the remaining information could be used to identify the individual.

Designated record set, under HIPAA, means a group of records maintained by or for a CE that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the CE to make decisions about individuals.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Electronic Health Record (EHR), as used in HIPAA, means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

FERPA means the Family Educational Rights and Privacy Act codified at 20 U.S.C. § 1232g with regulations at 34 C.F.R. § Part 99.

Functional Standards means the standards developed by CDC to identify operational, programmatic, and technical capacities that all IIS should achieve by the end of 2017.

Health Information Organization (HIO) means an organization that provides the capability to move clinical information electronically between disparate health care information systems while maintaining the meaning of the information being exchanged. Note that HIO is not defined in HIPAA.

HIPAA means the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, as amended.

Hybrid entity, under HIPAA, means a single legal entity and that conducts both covered and non-covered functions under HIPAA.

Individually identifiable information, under HIPAA, is information that identifies an individual or can reasonably be anticipated to be used to identify an individual.

Limited data set (LDS), under HIPAA, is PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.

Memorandum of understanding (MOU), under HIPAA, means an agreement between two (or more) governmental agencies establishing the responsibilities of each with respect to PHI. A MOU satisfies the requirements under HIPAA for a BAA between the governmental entities.

Minimum necessary, under HIPAA, means reasonable efforts of a CE to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

Notice of privacy practices (NPP), under HIPAA, means adequate notice of how a CE may use and disclose protected health information about the individual, as well as his or her rights and the CE's obligations with respect to that information.

Office of Civil Rights (OCR) is the U.S. Department of Health and Human Services agency that implements and enforces HIPAA.

Opt-in (or explicit consent) means that information is included in the IIS if the parent/individual explicitly consents (written or verbal) to participation in the IIS.

Opt-out (or implied consent) means that information is automatically included in the IIS unless a parent/individual requests (written or verbal) otherwise.

Parent is a person who can legally give consent for a child's immunization.

Protected health information (PHI), under HIPAA, is individually identifiable health information held or transmitted by a CE or its BA, in any form or medium, whether electronic, on paper, or oral.

Privacy is the legal right of an individual to limit access by others to some aspect of the person.

Privacy Rule means the regulation (Standards for Privacy of Individually Identifiable Health Information) issued by the U.S. Department of Health and Human Services ("HHS") to implement a requirement of HIPAA See 45 C.F.R. § Part 160 and Part 164, Subparts A and E

Public health authority, under HIPAA, means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from a public agency that is responsible for public health matters as part of its official mandate.

Purging information is one method to comply with an opt-out request. The IIS does not include information about the individual in the IIS or deletes information in the IIS. The purging can be of vaccination information and/or demographic information, and can be of some or all vaccination information and/or demographic information, as determined by applicable state, local and territorial laws.

Read-only access is a type of access to the IIS that allows an authorized user to view specified information in the IIS. Users with read-only access are not able to add, delete, or alter any information in the IIS.

Research, under HIPAA, means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Restricting access is one method to comply with an opt-out request. The IIS retains demographic and/or immunization information relating to the person who has made an opt-out request in the IIS. Use and disclosure of the information is restricted to limited people and organizations in accordance with applicable state, local and territorial laws, for example, for the IIS to perform certain functions and/or to the entity that provided health care to the individual.

Reminder/recall notice is a communication to a parent/individual/provider about immunizations due.

Security is a set of administrative, physical, technical and organizational safeguards designed to protect the IIS against unwarranted disclosure, modification, or destruction.

Security policy is a written policy applicable to the information in the IIS that sets forth policies and procedures to protect the security of the information in the IIS in accordance with applicable federal, state, local or territorial laws.

Site agreement defines the terms under which an IIS can disclose information to an organization and in which the organization agrees to abide by IIS confidentiality policies.

Treatment, Payment and Healthcare Operations (TPO), under HIPAA:

1. Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation and referral.
2. Payment includes activities of a health care provider and health plans relating to payment or reimbursement for health care services.
3. Health care operations include a CE's administrative, financial, and quality improvement activities that are essential to maintaining the entity's business and supporting treatment and payment transactions. Health care operations include the following activities: 1) conducting quality assessment and improvement activities, including outcome evaluation and development of clinical guidelines, so long as generalized knowledge is not the primary purpose of any studies resulting from such activities; 2) population-based activities relating to improving health or reducing health care costs, protocol development, and case management and care coordination; 3) activities involving accreditation, certification, and licensing, and 4) business management and general administrative activities of the entity, including: de-identifying PHI and creating a limited data set.

Use, under HIPAA, means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User agreement defines the terms under which an IIS can disclose information to individuals and the individual agrees to abide by IIS confidentiality policies.

Appendix E. Acronyms

Table 9. List of acronyms

Acronyms	Description
BA	Business Agreement
BAA	Business Associate Agreement
CE	CE
DUA	Data Use Agreement
EHR	Electronic Health Record
FERPA	Family Educational Rights and Privacy Act
HIO	Health Information Organization
HHS	United States Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IIS	Immunization Information System
LDS	Limited Data Set
MOU	Memorandum of Understanding
MU	Meaningful Use
NPP	Notice of Privacy Practices
OCR	Office Civil Rights within the United States Department of Health and Human Services
PHI	Protected Health Information
TPO	Treatment, Payment and Healthcare Operations

Appendix F. List of Resources

HIPAA Resources

HIPAA law: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

HIPAA rules: https://www.gpo.gov/fdsys/pkg/C.F.R.-2007-title45-vol1/pdf/C.F.R.-2007-title45-vol1.pdf, https://www.gpo.gov/fdsys/pkg/C.F.R.-2007-title45-vol1/content-detail.html and https://www.gpo.gov/fdsys/pkg/C.F.R.-2007-title45-vol1/content-detail.html.
An unofficial version of the combined rules implementing HIPPA (Omnibus Rule) is located at http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

HIPAA Privacy Rule and Public Health, Guidance from CDC and the U.S. Department of Health and Human Services, MMWR, April 11, 2003 / 52;1-12, http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm.

Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services Office for Civil Rights Health IT.gov Privacy and Security, Health IT Privacy and Security website. Resources, including tools, guidance documents, and educational materials intended to help integrate HIPAA and other federal health information privacy and security into practice.
https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources.

United States Department of Health and Human Services, Office of Civil Rights, Health Information Privacy website, http://www.hhs.gov/hipaa.

FERPA Resources

"Family Educational Rights and Privacy Act (FERPA) and the Disclosure of Student Information Related to Emergencies and Disasters," June 2010, available at http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-disaster-guidance.pdf.

FERPA statute: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf.

FERPA regulations: http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

Guidance on FERPA and public health, in both emergency and non-emergency situations.
http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-h1n1.pdf. Includes a model parental consent form.

Letter to Alabama Department of Education Regarding Disclosure of Immunization Records, dated February 25, 2004, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/alhippaa.html.

Letter to University of New Mexico re: Applicability of FERPA to Health and other State Reporting Requirements, dated November 29, 2004, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/baiseunmslc.html.

United States Department of Education Family Policy Compliance Office, FERPA website,
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

General Resources

Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap SUPPLEMENTAL MATERIALS Version 1.0, https://www.healthit.gov/sites/default/files/hie-interoperability/Interoperibility-Road-Map-Supplemental.pdf.

Emergency authority and immunity toolkit, Association of State and Territorial Health Officers, Legal preparedness series emergency authority and immunity toolkit, Emergency Declarations and Authorities Fact Sheet, http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Authority-and-Immunity-Toolkit/Emergency-Declarations-and-Authorities-Fact-Sheet.

Health Information and the Law, a project of the George Washington University Hirsh Health Law and Privacy Program and the Robert Wood Johnson Foundation website. Resource for state privacy laws. http://www.healthinfolaw.org/state.

Martin, Daniel W.; Lowery, N. Elaine; Brand, Bill; Gold, Rebecca; Horlick, Gail, Immunization Information Systems: A Decade of Progress in Law and Policy, Journal of Public Health Management & Practice, May/June 2015, Vol. 21, Issue 3, pp 296-303. http://journals.lww.com/jphmp/Fulltext/2015/05000/Immunization_Information_Systems___A_Decade_of.10.aspx.

Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information, Version 2.0, April 2015, https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services Office for Civil Rights Health IT.gov Privacy and Security, Health IT Privacy and Security website. Resource for state laws focusing on interoperability at https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations/state-hit-policy-levers-compendium.

State and Federal Consent Laws Affecting Interstate Health Information Exchange, March 2011, A technical report commissioned by the National Governors Association Center for Best Practices, http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF.

Appendix G. Master Checklist for Confidentiality and Privacy Considerations for IIS Policies and Procedures

IIS can use the following checklist to assist in developing confidentiality policies and procedures. IIS should refer to the entire document for more detailed information, particularly Chapter 3. Privacy and Confidentiality in IIS and Chapter 4. IIS Confidentiality Policies and Procedures. This checklist may not include all relevant confidentiality and privacy considerations. Each IIS should consult with local authorities to ensure that its confidentiality policies are in accordance with applicable federal, state, local and territorial laws.

1. **General provisions**
   Confidentiality policies can:
   - ✔ Contain citations to applicable federal, state, local and territorial laws. If the IIS is governed by HIPAA, state that HIPAA applies
   - ✔ Be available to anyone who asks for them, for example, easily accessible through the IIS website
   - ✔ Be reviewed regularly (for example, annually) by legal counsel or other appropriate authority to ensure that they are consistent with applicable federal, state, local and territorial laws
   - ✔ Apply to everyone who has authorized use of information in the IIS, or authorized access to information in the IIS, including workforce, consultants, authorized users and business associates
   - ✔ Apply to all individually identifiable information in all formats including paper-based and electronic records
   - ✔ Include a point of contact at IIS
2. **Authority to operate IIS**
   - ✔ Examine state, local and territorial laws to determine authority to operate the IIS for each age group included in the IIS
3. **Notice to individuals of inclusion of information in the IIS and/or notice of privacy practices**
   - ✔ Determine if a notice is required, for example, HIPAA applies or state, local and territorial laws requires a notice
   - ✔ If notice is required, determine:
     - Who must provide notice
     - Notice contents
     - Notice timing
     - Form of notice (e.g., written)
4. **Choice (Consent)**
   - ✔ If HIPAA applies, determine if proposed disclosure is permitted without authorization:
     - To an IIS (HIPAA public health exception)
     - To an individual (HIPAA exception)
     - To health care provider (HIPAA exception for treatment purposes)
     - To researcher (HIPAA exception with limitations)
     - Other
   - ✔ Examine state, local and territorial laws for consent requirements for each age group included in the IIS (childhood, adolescent, adult).
     - Examine following types of laws:
       - Laws authorizing operation of an IIS
       - Specific laws/policies governing vital records
       - Laws defining scope of practice laws for the provider type
         - Traditional (for example, pediatricians)
         - Non-traditional (for example, pharmacies)
     - Determine the type of consent (if any) required for each age group in the IIS:
       - No consent required
       - Implicit consent with opt-out
       - No consent; with opt-out
       - No consent; no opt-out
       - Explicit consent
     - Determine requirements for consent/withdrawal (if allowed):
       - Oral or written consent
       - How to withdraw consent
       - Type of documentation
       - Who retains documentation
   - ✔ Determine effect of opt-out on information in the IIS:
     - Purge
     - Limit access

5. **Permitted use/disclosure of information by the IIS**
   - ✔ Determine if HIPAA applies/has applicable exception to authorization
   - ✔ Examine state, local and territorial laws to determine:
     - Permitted persons/entities for use/disclosure of IIS information by age group included in the IIS
     - Permitted purposes for use/disclosure of IIS information by age group in the IIS and by type of person/entity
   - ✔ Examples of permitted persons/entities for use/disclosure:
     - To the individual
     - Research
     - Schools
     - Health care providers
6. **Data retention and disposal**
   - ✔ Determine if HIPAA applies
     - General six-year retention period
   - ✔ Examine state, local and territorial laws to determine:
     - What to retain
     - Retention time
7. **Rights of individuals to access, inspect and amend**
   - ✔ Determine if HIPAA applies
     - Individuals have rights to access, inspect and request amendment of their information in a designated record set
   - ✔ Examine state, local and territorial laws to determine individual's rights to access, inspect and amend
8. **Breach notification**
   - ✔ If HIPAA applies, notice to:
     - affected individuals
     - the Secretary of HHS
     - sometimes to media
     - the CE if the breach is at a business associate
   - ✔ Determine if state, local and territorial laws contains breach notification requirements
9. **Sanctions**
   - ✔ Determine if HIPAA applies
     - Civil and criminal penalties
   - ✔ Examine state, local and territorial laws to determine sanctions for violations of state, local and territorial laws
10. **Ensure compliance with Confidentiality Policies**
    - ✔ Site Agreement provisions
      - Appropriate authorities will review the site agreement regularly (e.g., at least annually) to ensure continuing compliance with federal, state, local and territorial laws
      - The site agrees to:
        - enforce the IIS confidentiality policies
        - issue passwords to individuals and to enforce prohibitions on sharing passwords
        - inform the IIS within a reasonable amount of time after any authorized IIS user becomes ineligible to be an IIS authorized user
        - keep an audit trail of all persons who access/use information received from the IIS
        - notify the IIS immediately about any unauthorized use/disclosure of IIS information
    - ✔ User Agreement
      - Appropriate authorities will review the user agreement regularly (e.g., at least annually) to ensure continuing compliance with federal, state, local and territorial laws
      - The individual agrees to:
        - comply with the IIS confidentiality policies and federal, state, local or territorial laws with respect to IIS information
        - only access information that the individual has a need to know to perform her/his duties
        - not share her/his IIS password with anyone
        - notify the IIS immediately about any unauthorized use/disclosure of IIS information

Appendix H. IIS Sample Forms

Figure 5. Provider Site Enrollment Form Sample (from Massachusetts IIS)

Massachusetts Immunization Information System

MIIS

PROVIDER SITE ENROLLMENT AGREEMENT

The MIIS is an internet-based immunization registry operated by the Immunization Program of the Massachusetts Department of Public Health (MDPH). Enrolled health care providers can obtain immunization information for patients, including tracking and reminder/recall. Patient information is confidential and only available to the authorized users.

The MIIS is established and operated under the authority of M.G.L. Chapter 111, Section 24M.

As a condition of participating in the MIIS, the Provider enters into this agreement with MDPH, and agrees to the following:

- The Provider agrees to use the MIIS only for the immunization needs of patients. The Provider and his/her staff will access the registry only to:
  - assure adequate immunization,
  - avoid unnecessary immunizations,
  - confirm compliance with immunization requirements,
  - control disease outbreaks,
  - conduct ongoing or special immunization coverage assessments, and
  - comply with reporting requirements.

- The Provider shall abide by the requirements in the attached MIIS Individual User Agreement and Confidentiality Statement, which is incorporated by reference into this agreement. Each staff member seeking access to the MIIS must sign the Individual User Agreement and Confidentiality Statement, which must be kept in the employee's personnel file.

- All information in the system is confidential and shall be considered by users to be “Personal Health Information” (PHI) as defined and protected in the Health Insurance Portability and Accountability Act. Users shall comply with the requirements of HIPAA, the attached Confidentiality Statement, and any other applicable confidentiality laws. The Provider will take all reasonable steps to assure employee compliance with these confidentiality requirements.

- The Provider shall inform patients, parents or guardians about the system, as described in the MIIS Policy Statement. The MIIS Fact Sheet for Parents and Patients and MIIS posters shall be made readily available to parents and patients.

- The Provider shall promptly submit via data exchange or enter into the MIIS specified demographic and immunization information about patients receiving immunizations, striving for submission within one week after immunization administration.

- The Provider shall allow the patient, parent or guardian to inspect, copy, and if necessary, amend or correct an immunization record if he/she demonstrates that such record is incorrect. This corrected information shall be entered into the MIIS.

If this agreement is violated by any user, MDPH reserves the right to terminate access to the system.

1 of 2

Please initial here:

PROVIDER SITE ENROLLMENT (*To participate in the Massachusetts Immunization Information System*)

Facility Name: _____

Site Name (if applicable): _____

Is this site an enrolled provider with the MDPH Vaccine Unit? ☐ YES ☐ NO If yes, list PIN # _____

Site Street Address: _____

Site City and State: _____ Site Zip Code: _____

Phone: _____ FAX: _____ E-Mail: _____

Primary Immunization Contact: _____

Title: _____

Phone: _____ E-Mail: _____

Primary Technical/Computer Contact: _____

Title: _____

Phone: _____ E-Mail: _____

Supervising Physician, Site Manager, or Designee Full Name, Title and Degree:

_____

Facility National Provider Identifier (NPI): _____

Organization Type (please circle): ☐ Private Practice ☐ Community Health Center ☐ Public School

☐ Private School ☐ Hospital ☐ Child Care Center ☐ Nursing Facility ☐Board of Health

Other: _____

How will you primarily be submitting data to the MIIS: ☐ Direct Data Entry ☐ Electronic Data Exchange (HL7)

Does your facility use an electronic health record? ☐ YES ☐ NO

If yes, please list electronic health record type: _____

Signing this form signifies that you are in agreement with the items outlined on page one (1) of this form. Please sign, keep a copy for yourself, and fax the form to 617-983-4301 or mail the original to the Massachusetts Department of Public Health, Immunization Program - MIIS, 305 South Street Suite 560, Jamaica Plain, MA 02130.

_____ _____

Signature of Supervising Physician, Site Manager or Designee Date

_____

Printed Name and Title

Figure 6. User Agreement and Confidentiality Statement Sample (from Massachusetts IIS)

Massachusetts Immunization Information System

MIIS

MIIS INDIVIDUAL USER AGREEMENT AND CONFIDENTIALITY STATEMENT

Part 1: Purpose

The MIIS is an internet-based immunization registry operated by the Immunization Program of the Massachusetts Department of Public Health (MDPH) under the authority of M.G.L. Chapter 111, Section 24M. Enrolled health care providers can obtain immunization information for patients, including tracking and reminder/recall. Patient information is confidential and only available to the authorized users.

This agreement establishes the terms and conditions under which authorized users may obtain access to MIIS data. Violation of the terms of this agreement shall provide grounds for terminating access to the MIIS as MDPH deems appropriate.

This agreement details the responsibilities of the authorized user with regard to:

1.1 Enrolling and participating in the MIIS
1.2 Confidentiality
1.3 Security Procedures

1.1 Enrolling and Participating in the MIIS

A. Eligible Participants

The following sites and individual providers may be authorized by MDPH to use the MIIS:

a. Licensed health care providers providing direct care to the individual patient,
b. Elementary and secondary school nurses and registration officials who require proof of immunization for school enrollment and disease control,
c. Local boards of health for disease prevention and control,
d. Women Infants and Children (WIC) nutrition program staff who administer WIC benefits to eligible pregnant women, infants and children, and
e. Staff of state agencies or state programs whose duties include education and outreach related to the improvement of immunization coverage among their clients.

B. Provider Enrollment

In order to access the MIIS, every user must be part of a provider site that is registered with MDPH. To register, a site must complete the Provider Site Enrollment Agreement. Access is limited to sites that provide immunization services or agencies that ensure that individuals are up to date with their immunizations.

The Provider Site Enrollment Agreement must be signed by a supervising physician, site manager or designee, who assumes responsibility for the proper use and protection of registry data at their site. Each site must designate authorized users, who will be issued user names and passwords. Only authorized users shall be permitted access to the site.

The site manager shall ensure that each authorized user reads and signs this form, including the Confidentiality Statement in section 4. This form must be completed prior to receiving a User ID and password. **The signed copy of this form is to be kept in the Employee's Personnel File.**

1 of 3 Please initial here:

The Site Manager will notify the MIIS Help Desk promptly when accounts need to be deleted or created due to changes in personnel. Users who willfully misuse information contained in the registry will have their access immediately restricted by MDPH. To delete a User from the site, the site manager shall use the Remove User Form which should be faxed to the MIIS program at 617-983-4301 within one week of the User's last day of employment.

Where there is reason to believe that a breach of this agreement or a patient's confidentiality has occurred, the site manager or supervising physician shall promptly file an incident report with the MIIS Program. Following investigation, the MIIS program will take appropriate action, including termination of access.

C. Individual User Agreement

Authorized users of the MIIS must agree to:

a. Provide patients, parents, or guardians with the MIIS Fact Sheet and enter new patients, if not already in the MIIS, at their first immunization encounter,
b. Promptly enter into the MIIS specified demographic and immunization information about patients receiving immunizations, striving for submission within one week after immunization administration,
c. Submit, at a minimum, all required data elements, as indicated with an asterisk in the application,
d. Report available information on past immunizations, if not already reported by another provider, and
e. Provide MIIS generated records to the parent/guardian or individual upon request and without cost and, if necessary, amend or correct the immunization record if s/he demonstrates that the record is incorrect by providing verifiable documentation of immunization.

1.2 Confidentiality Statement

A. All authorized users of the MIIS must agree to:

a. Access, copy and use patient specific information only as needed to ensure adequate, up to date immunizations, avoid unnecessary immunizations, control disease outbreaks, or as otherwise needed to meet or ensure compliance with immunization requirements for that patient. Licensed health care providers may only access records of patients for whom they are clinically or contractually responsible.
b. Handle information or documents obtained through the MIIS in a confidential manner similar to handling any other confidential medical information. All information in the system when accessed by an authorized user should be regarded as "Personal Health Information (PHI)", as described and protected in the Health Insurance Portability and Accountability Act.
c. Acknowledge that all transactions are logged and may be subject to audit.
d. Carefully safeguard access privileges and passwords.
e. Properly exit the MIIS when the Authorized User is not present at the computer by logging off and closing the browser when finished with an MIIS session.
f. Promptly report any threat or violation of MIIS confidentiality or security to the site manager or MDPH.
g. Permit access to researchers or use data for research only if approved by MDPH pursuant to M.G.L. c. 111, s.24 and in accordance with c. 111, s. 24M.

B. All authorized users agree not to:

a. Share their user name and password with anyone,
b. Permit other persons to access the MIIS by using another person's login and password,
c. Enter inaccurate data intentionally, or alter or falsify any document or data obtained through the MIIS,
d. Remove from a job site or copy any document or computer record containing confidential information unless specifically authorized to do so by the site manager and only if required in the course of official duties, and
e. Use data in the system to discriminate, threaten, or take any adverse action with respect to a data subject.

1.3 Security Procedures

All enrolled sites shall maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of health information, in accordance with any MDPH guidelines. Immunization Program staff may conduct periodic assessments on privacy and security policies.

 Please initial here:

Part 2: Signature

I have read, agree and will abide by the terms of this User Agreement and Confidentiality Statement. I understand and accept these terms. Further, I understand that any violation of these provisions may result in investigation, termination of my access privileges, or other action deemed appropriate by MDPH.

(ALL FIELDS ARE REQUIRED AND MUST BE FILLED IN)

Applicant Full Name (First Name, Middle Initial, Last Name):
Date of Birth (MM/DD/YY):
Facility Name:
Supervising Physician's or Site Manager Full Name and Degree:
Facility National Provider Identifier (NPI):
Facility Address: Street _____ City _____ State _____ Zip ____
Phone: Fax:
Applicant's Individual E-Mail Address: (Group or mulit-user email not acceptable)
Supervising Physician or Site Manager Signature: Date Signed:
Applicant Signature: Date Signed:

Figure 7. Regulations for Massachusetts IIS (from Massachusetts IIS)

105 CMR: DEPARTMENT OF PUBLIC HEALTH

105 CMR 222.000: MASSACHUSETTS IMMUNIZATION INFORMATION SYSTEM

Section

222.001: Purpose

The purpose of 105 CMR 222.000 is to facilitate and promote the use of the Massachusetts Immunization Information System (MIIS) to help improve immunization coverage among all individuals in the Commonwealth.

222.002: Scope

105 CMR 222.000 applies to all health care providers licensed in the Commonwealth who administer immunizations in Massachusetts to any person, whether or not that person is a resident of the Commonwealth, and any entity that accesses the MIIS.

222.003: Definitions

Department means the Massachusetts Department of Public Health.

EHR means an electronic health record.

Electronic Data Exchange means the electronic interchange of information or data using a standardized format that allows one entity to send information to another electronically rather than with paper.

GUI means a web-based graphical user interface.

Health Care Provider means a health care professional who administers immunizations and is licensed under M.G.L. c. 112 and pharmacists authorized by 105 CMR 700.004(B)(6) to dispense vaccine by administration.

Immunization means a vaccine or immunoglobulin, identified on a list maintained by the Department that introduces active or passive immunity to a specific disease or group of diseases.

MIIS means the Massachusetts Immunization Information System.

MIIS Fact Sheet means the MIIS Fact Sheet for Parents and Parents

MRVRS means the Massachusetts Registry of Vital Records and Statistics.

Objection to Data Sharing means an individual's immunization information will be accessible only to Department staff and the provider that entered the immunization information.

Objection Form means a mechanism as determined by the Department by which an individual may indicate an objection to sharing immunization information across providers that access the MIIS.

VIS means Vaccine Information Statements, which are information sheets produced by the Centers for Disease Control and Prevention (CDC) that explain to vaccine recipients, their parents, or their legal representatives the risks and benefits of a vaccine.

1/2/15 105 CMR - 1202.1

222.003: continued

VFC means the federal Vaccines For Children Program.

222.100: Health Care Provider Immunization Information Reporting

(A) Health care providers shall report all new immunizations either through the GUI or by data exchange within seven days of immunization administration.

(B) Health care provider sites that perform data exchange shall comply with all electronic data exchange specifications required by the Department.

(C) Health care provider sites performing electronic data exchange shall send complete immunization records with all new immunizations being reported to the system. If sites are unable to send complete records, they may perform a one-time historical upload of records into the MIIS in a form and manner determined by the Department.

(D) Data for each individual reported through the GUI shall include at a minimum:
(1) For both current and historical immunizations, the full first and last name and date of birth of the individual, immunization type, and date of immunization administration;
(2) For current immunizations, VFC status, individual's current home address, immunization manufacturer and lot number, name, address, and title of the person administering the immunization, edition date printed on the appropriate VIS, and date the VIS was given to the individual or the individual's parents/legal representative (if younger than 18 years old); and
(3) Any other information as determined by the Department.

222.105: Duty to Inform

(A) Providers shall explain to individuals, or the parent or legal guardian of an individual under 18 years of age, the MIIS reporting procedures and requirements for immunization information for all individuals to the MIIS, including the right to object to data sharing, as described in 105 CMR 222.105(C).

(B) Written materials developed by the Department for this purpose may include: MIIS Fact Sheet, posters, sample language for individual registration forms, sample provider email or template letters for informing individuals, MIIS Objection (or Withdrawal of Objection) Form. These materials will be maintained and updated by the Department.

(C) Objection/Withdrawal of Objection Procedures.
(1) If an individual, or the parent or guardian of an individual younger than 18 years old, chooses to object to data sharing (or withdraw objection to data sharing) in the MIIS, the individual must complete the Objection Form and submit it either to his or her health care provider or directly to the Department.
(2) If an Objection Form is received directly by a provider, the provider must fax the form to the Department within 24 hours of receipt. Providers must also change the data sharing status of the individual in the GUI in order to ensure the Objection or Withdrawal of Objection is implemented within the system immediately, as practical.
(3) The records of an individual whose data sharing is changed from "Yes" or "Unknown" to "No" will be accessible only by the provider site that entered the immunization information.
(4) An individual who has objected to data sharing, but whose name is not yet in the MIIS, will be added to the system and will have data sharing status set to "No" by the Department.

(D) All birth hospitals/facilities shall also inform the individual's parent or guardian of the electronic data transmission of all immunizations provided to newborns from MRVRS to MIIS.

222.200: Provider Enrollment

(A) Health care provider sites shall review and complete the Provider Site Enrollment Agreement prior to enrolling individual users at their site in the MIIS.

222.200: continued

(B) Health care providers shall enroll and agree to comply with all terms and conditions set forth in the MIIS Individual User Agreement and Confidentiality Statement prior to receiving access to the MIIS either through the GUI or electronic data exchange. Signed individual user agreements shall be sent to Department and copies maintained at the provider site.

(C) Department may at any time revoke access to the MIIS from any user who fails to comply with the MIIS Individual User Agreement and Confidentiality Statement.

222.205: System Access and Confidentiality

(A) Immunization information shall be released from the MIIS only to the following individuals and agencies without further expressed consent of the individual or the individual's parent or guardian unless the individual or the individual's parent or guardian has objected to data sharing:

(1) Licensed health care providers and their staff providing direct care to the individual patient;

(2) Elementary and secondary school nurses and registration officials who require proof of immunization for school enrollment and disease control;

(3) Local boards of health for disease prevention and control;

(4) Women Infants and Children (WIC) nutrition program staff who administer WIC benefits to eligible infants and children; and

(5) Staff of state agencies or state programs whose duties include education and outreach related to the improvement of immunization coverage rates among their clients.

(B) In accordance with the MIIS Individual User Agreement and Confidentiality Statement, all users of the MIIS must agree to access immunization information solely for the purpose of ensuring that individuals are up to date on the recommended immunization schedule, in compliance with school entry immunization requirements, for disease control and prevention, or for the improvement of immunization coverage rates of their clients or the public.

(C) Access by Department Staff. Authorized Department staff may have access to all records in the system including those for which data sharing status is set to "No".

(D) Access by Researchers. Research requests shall be submitted through the Department's research proposal submission system and reviewed by designated Department staff. Researchers granted approval shall sign the MIIS Individual User Agreement and Confidentiality Statement.

(E) Access by Non-health Care Providers. Non-health care providers who may be granted access to the system for "view only" and/or report generating privileges shall complete a site and an individual agreement and agree to comply by the same terms and conditions that apply to health care providers.

(F) Protection from Subpoena and Public Record Requests. Information contained in the MIIS does not constitute a public record, is not subject to subpoena or court order, and is not admissible as evidence in any action of any kind before a court, tribunal, agency, board, or person.

222.300: Requests to Amend Records and Access Records by Individuals

(A) Incorrect information may be amended by an individual's health care provider or by any health care provider if the individual has not objected to data sharing in the MIIS.

(B) Requests for record amendments may also be made directly to the Department in writing in a form and manner determined by the Department.

(C) Requests for copies of records by individuals should be made to their health care provider. Such requests may be made in person and the health care provider filling the request shall validate the individual's identity, and in the case of a minor's record, validate that the individual is the legal guardian or parent of the minor. Requests may also be made directly to the Department in writing in a form and manner determined by the Department.

222.305: Requests for List of Those Who Have Accessed Records

Requests for a record of all MIIS users that have accessed an individual's immunization information shall be made in writing in a form and manner determined by the Department.

222.400: Compliance Schedule

All health care providers licensed in the Commonwealth who administer immunizations in Massachusetts to any person, whether or not that person is a resident of the Commonwealth, shall be in compliance with 105 CMR 222.000 according to a schedule to be determined and distributed by the Department.

REGULATORY AUTHORITY

105 CMR 222.000: M.G.L. c. 111, §§ 3 and 24M.

Figure 8. Provider Site Agreement Sample (from North Dakota IIS)

North Dakota Department of Health
Immunization Program
2635 East Main Ave., P.O. Box 5520
Bismarck, ND 58506-5520
Fax Number: 701.328.0355
Web: www.ndhealth.gov/immunize

Provider Site Agreement - North Dakota Immunization Information System

The North Dakota Immunization Information System (NDIIS) is a confidential, electronic system that collects immunization data for all North Dakotans. North Dakota Century Code[1] and Administrative Rules[2] cover collection and release of information in the NDIIS. By law, information is confidential and can only be shared with authorized users, including healthcare providers, local public health units, schools, childcare facilities, individuals themselves or their parent/guardian if the individual is younger than 18. North Dakota Century Code mandates that providers share childhood immunization information with the NDIIS; patient/parent/guardian consent is not required. Adult information should also be entered into the NDIIS; however, adults can opt out of the NDIIS. The NDIIS is covered under the federal Health Insurance Portability and Accountability Act (HIPAA)[3] and complies with all HIPAA rules and regulations and the North Dakota Department of Health is obligated to report any HIPAA violation to the appropriate authority.

As a condition of receiving immunization information from the NDIIS as a provider, users must agree to the following:

1. Only access immunization information in the NDIIS for individuals under their care.
2. Read and abide by the NDIIS Confidentiality Policy.
3. Abide by all security policies and procedures, including safeguarding username(s) and password(s) against unauthorized use.

Each provider site must designate a Site Administrator who must agree to the following:

1. Be the sole authority to authorize new NDIIS users for their provider site.
2. Notify THOR support within one week of staff leaving facility to deactivate users who are no longer affiliated with this site or approved to have access to NDIIS.
3. Ensure that each staff member requiring access has their own username and password, so that login information is not shared between users.
4. Be the point of contact for account verifications, system alerts and policy changes.
5. Be responsible for ensuring that users comply with all applicable laws, regulations and NDIIS policies.
6. Ensure NDIIS users have appropriate training on the proper use of the NDIIS.
7. Notify the NDDoH at least one week in advance that I am no longer able to perform these tasks to allow for the transition to a new NDIIS Site Administrator.

Failure to abide by this agreement may result in immediate termination, suspension or revocation of access to the NDIIS. Misuse of NDIIS data will be reported to the appropriate licensing body.

[1] North Dakota Century Code 23-01-05.3
[2] North Dakota Administrative Rule 33-06-05-01
[3] Health Insurance Portability and Accountability Ave (HIPAA), 45 C.F.R. Parts 160 and 164

NORTH DAKOTA
DEPARTMENT of HEALTH

Provider Site Information		
Name of Provider Site:		
Parent Organization (if any):		NDIIS Provider Pin:
Physical Address:		
City:	State:	ZIP Code:
Mailing Address (if different from physical address):		
City:	State:	Zip Code:
Phone Number:	Fax Number (if requested to be sent via fax):	

Site Administrator Information		
Site Administrator First Name:	Last Name:	
Title:	Phone:	Email:
Signature of Site Administrator:		

Site Authorized Representative (e.g. Managing Physician, CEO)		
First Name:	Last Name:	
Title:	Phone:	Email:
Signature of Authorized Representative:		

North Dakota Department of Health *(For Office Use Only)*		
Date Received:	Date Executed:	Initials:

Figure 9. User Agreement Sample 1 (from North Dakota IIS)

Terms and Conditions for use of 'The Healthcare On-line Resource' (THOR)

Read the following terms and conditions carefully before continuing. User must accept these terms and conditions to obtain access to the THOR System. If user does not agree to these terms and conditions, user will not be able to use the THOR System. It is suggested that user check these terms periodically for changes. The terms can be accessed from the link at the bottom of the THOR main menu. If the THOR System is accessed after changes to these terms and conditions are posted, user will be deemed to have accepted any changes.

Terms and Conditions as of: January 1, 2014.

User Access

User shall have access to such applications as Blue Cross Blue Shield of North Dakota (BCBSND) makes available through the THOR System. BCBSND reserves the right to determine the applications and level of access granted to each user.

BCBSND may, without advance notice or liability, add, discontinue, or revise any aspect of the THOR System, including without limitation such aspects as scope of service, availability of service, time of service availability, or the hardware and/or software required for user to access and use the THOR applications. BCBSND will make reasonable efforts to provide user with advance notice of such events when practicable.

User Equipment and Remote Connection Charges

User shall be responsible for obtaining and maintaining, at users' own expense, all computer hardware, software, communication equipment and access lines necessary to access and utilize the THOR System.

Data Security

The THOR System uses the following security measures to ensure the security of data being transferred:

The THOR System uses some of the most secure forms of online communications available, including Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol, and a reputable trusted X.509 Certificate

The application requires the user to have IE 6 or greater with a minimum of 128-bit encryption (cypher-strength).

User Codes and Passwords

Role based security is enforced to ensure information is accessible on a need to know basis. User access is restricted to assigned BCBSND provider identification numbers.

User is responsible for maintaining the confidentiality of the user code and password and is responsible for all activities resulting from their use, including unauthorized use. User is responsible to immediately notify 'THOR Support Services' when discontinuing use of the THOR System, or in the event the user code and password are compromised or abused.

Conduct of User

User agrees to use the THOR System only for lawful purposes. User will not post or transmit on or through the THOR System any libelous, obscene, or otherwise unlawful information of any kind, and user will not engage in any conduct involving the THOR System that would constitute a criminal offense or give rise to civil liability under any local, state, federal or other law or regulation, including, but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). User will not upload, post, reproduce or distribute to or through the THOR System any material protected by copyright, privacy or other proprietary right without first obtaining the written permission of the owner thereof. User acknowledges that the THOR System contains copyrighted and other proprietary and confidential information and material, and user will respect all such proprietary rights and take such precautions as may be reasonably necessary to protect private, confidential and other proprietary information and material from unauthorized use or disclosure.

User is responsible for compliance with all policies and procedures set forth in newsletters and bulletins published by payors or government agencies.

Availability of Benefits

The data presented is not a guarantee of benefits. Benefits are only available for medically appropriate and necessary treatment that is covered according to the terms of the benefit plan and subject to the patient's eligibility on the date of service. Benefits will be denied if the member is not eligible on the date of service.

Accuracy and Validity of Information and Opinions

BCBSND will make reasonable efforts to ensure that information it contributes to the THOR System is timely and accurate. However, BCBSND does not warrant and assumes no responsibility whatsoever for the timeliness, accuracy, reliability, completeness or usefulness of any statement, opinion, advice, service or other information contributed by any third party.

Monitoring of the THOR System

BCBSND may, in its discretion and without notice, monitor the THOR System and user's use thereof to determine and ensure compliance and to protect itself and other users of the THOR system from fraudulent, unlawful or abusive use, or for any other reason deemed necessary by BCBSND. BCBSND may also intercept and disclose any content, record, use or other information to the extent reasonably necessary to protect the rights of BCBSND, for mechanical or service quality control as permitted by law, or to comply with any law, regulation, or governmental request. BCBSND may also, in its discretion and without notice, review, edit, refuse to post or remove any material or information submitted or transmitted to the THOR System.

On-line Updates

BCBSND may, when feasible, update the THOR System either with or without notice to user. Such updates will occur automatically on-line upon user's signing into the THOR System or may occur pursuant to prompts, which appear on user's web screen during use of the THOR System. User hereby consents to the process of the on-line updates, waiving any and all claims for damages, etc., related thereto.

THOR System Maintenance

Planned availability to the THOR System will be 24 hours a day 7 days a week. The system will be brought down for occasional maintenance. To the extent possible, this maintenance will be scheduled on the weekends and off-hours when it will be least likely to cause an interruption in production. Notification of this downtime will be communicated to the user through the broadcast news messaging board on the THOR main menu.

THOR Support Services

A toll free, telephone support line to assist users with the THOR System will be available. THOR Support Services hours are 8:00 a.m. to 4:30 p.m. central standard time. These hours are also posted on the THOR bulletin board.

Copyright Protection

The THOR System and the content provide therein, are protected by copyright. All rights in the pages, site content, graphics, and arrangement are owned by BCBSND. User is prohibited from modifying, copying, distributing, transmitting, displaying, publishing, selling, licensing, creating derivative works of or using any of the content from the THOR System for commercial or public purposes.

Trade Marks and Service Marks

BCBSND uses the “Blue Cross Blue Shield” trademarks and service marks under license from the Blue Cross and Blue Shield Association. Any use of these trademarks or service marks, without the prior written consent of BCBSND and/or BCBSA, is expressly prohibited. All other trademarks and/or service marks used herein are the property of their respective owners.

Applicability of State and Federal Laws

All products and services provided through the THOR System are subject to all applicable state and federal laws. This includes, but is not limited to, all laws related to insurance, employee benefits, equal employment opportunity, and the Americans with Disabilities Act.

Users' Privacy

While BCBSND is committed to protecting the privacy of its members and others, it is possible that any transmission of data on or through the Internet may be intercepted, monitored, or downloaded by an unauthorized third party. To the extent allowed by state and federal law, BCBSND expressly disclaims any liability for any data transmitted by the user, intentionally or otherwise, over the Internet. USER ASSUMES ALL RISK FOR THE SENDING OF ANY INFORMATION, BY ANY MEANS, INTENTIONAL OR OTHERWISE, VIA THE INTERNET.

Judgement of the Provider

The professional judgement of the physician or other provider and the member’s discretion are the only factors in determining whether the member can, may or should receive such medical services and/or supplies. BCBSND's only responsibility is to determine whether benefits will be paid under a contract for health care.

DISCLAIMER OF WARRANTIES

EXCEPT AS EXPRESSLY PROVIDED ABOVE, THE THOR SYSTEM, AND INFORMATION AVAILABLE THROUGH THE THOR SYSTEM ARE FURNISHED BY BCBSND AND ACCEPTED BY USER "AS IS" AND "AS AVAILABLE", WITHOUT ANY WARRANTY WHATSOEVER. ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ARE SPECIFICALLY EXCLUDED AND DISCLAIMED. BCBSND DOES NOT WARRANT THAT THE THOR SYSTEM, OR INFORMATION OBTAINED THROUGH THE THOR SERVICES, WILL MEET USER'S REQUIREMENTS, THAT THE OPERATION OF THE THOR SYSTEM WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL FAILURES OF THE BCBSND THOR SYSTEM TO SUBSTANTIALLY CONFORM TO OR PERFORM SUBSTANTIALLY IN ACCORDANCE WITH BCBSND'S SPECIFICATIONS WILL BE CORRECTED. EXCEPT AS EXPRESSLY PROVIDED ABOVE AND IN SUCH WARRANTIES, IF ANY, AS MAY BE PROVIDED BY THIRD PARTY VENDORS OF EQUIPMENT OR SOFTWARE UTILIZED IN CONNECTION WITH THOR, THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE THOR SYSTEM, AND INFORMATION OBTAINED THROUGH THE THOR SYSTEM IS WITH USER.

Term and Termination

Either party may, at its election and in its sole discretion, terminate access to the THOR System. THOR Support may, at any time, terminate a user's access to any or all of the THOR applications without advance notice if the user has prolonged inactivity or commits any violation.

Entire Agreement

These terms and conditions set forth the entire agreement and understanding between BCBSND and user regarding the subject matter hereof and supersede any prior representations, advertisements, statements, proposals, negotiations, discussions, understandings, or agreements regarding the same subject matter. If user has entered into an Electronic Trading Partner Agreement with BCBSND, the terms of the Electronic Trading Partner Agreement remain in effect and are not superceded by this Agreement.

LIMITATION OF BCBSND LIABILITY

IN NO EVENT WILL BCBSND BE LIABLE TO USER OR ANY OTHER PERSON FOR ANY LOST PROFITS, LOST SAVINGS, LOST DATA, OR OTHER SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY INFORMATION, PRODUCT OR SERVICE FURNISHED OR TO BE FURNISHED BY BCBSND UNDER THIS AGREEMENT OR THE USE THEREOF, EVEN IF BCBSND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE, AND THE AGGREGATE LIABILITY OF BCBSND UPON ANY CLAIMS HOWSOEVER ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY INFORMATION, PRODUCTS OR SERVICES FURNISHED OR TO BE FURNISHED BY BCBSND UNDER THIS AGREEMENT WILL IN ANY EVENT BE ABSOLUTELY LIMITED TO THE AMOUNT PAID TO BCBSND BY USER UNDER THIS AGREEMENT; PROVIDED, HOWEVER, THAT NOTHING IN THIS AGREEMENT SHALL OPERATE TO RELIEVE BCBSND FROM LIABILITY FOR ITS OWN WILLFUL OR WANTON RECKLESSNESS OR INTENTIONAL TORTS.

Figure 10. User Agreement Sample 2 (from North Dakota IIS)

NORTH DAKOTA IMMUNIZATION INFORMATION SYSTEM
CONFIDENTIALITY POLICY AND USER AGREEMENT

The North Dakota Immunization Information System (NDIIS) is a confidential, population-based, computerized information system that attempts to collect vaccination data about all North Dakotans. The NDIIS is an important tool to increase and sustain high vaccination coverage by consolidating vaccination records of children from multiple providers and providing official vaccination forms and vaccination coverage assessments. Children are entered into the NDIIS at birth, through a linkage with electronic birth records. An NDIIS vaccination record also can be initiated by a health care provider at the time of a child's first immunization. The NDIIS has the capability of collecting vaccination data on adult patients, as well as children.

The NDIIS confidentiality policy provides for the disclosure and use of immunization information among health care providers, schools, childcare centers and publicly funded programs to meet statutory immunization requirements and to control disease outbreaks.

NDIIS is developed under the authority of the following provisions of the North Dakota Century Code: Title 23 Chapter 23-01-05.3, Immunization Data; Title 23, Chapter 23-07-17.1, Inoculation required before admission to school; and North Dakota Administrative Rule Chapter 33-06-05 School Immunization Requirements.

The purpose of this policy is to address the need to provide appropriate confidentiality protections to the information in the NDIIS. The confidentiality of the information must be distinguished from issues of privacy. Privacy is concerned with the control individuals exert over their personal information. Under NDIIS's policy, confidentiality is concerned with how the information provided to NDIIS by individuals is accessed, collected, stored, used and provided to other individuals and organizations. The responsibility of protecting confidentiality extends to anyone having access to information contained in the registry, whether it is accessed directly or indirectly through interoperability with a provider's electronic medical record or through the state's health information network.

NDIIS shall protect the privacy of registry participants and the confidentiality of information contained in registries. Patient and provider specific information in NDIIS is only available to the authorized users and the NDDoH.

SECTION I: PATIENT PARTICIPATION

1. A Patient's Right Not to Participate in the NDIIS

Participation in the NDIIS is required by state law for children according to North Dakota Century Code 23-01-05.3.

An adult may choose to be excluded from the NDIIS; thereby limiting future access to his/her immunization records through the NDIIS, by notifying the healthcare provider. It is the responsibility of the healthcare provider to notify adult patients that their information will be added to the NDIIS. If the patient chooses to opt-out of the NDIIS, it is the responsibility of the healthcare provider to mark the "opt out" box on the NDIIS client maintenance screen to ensure that the patient has been opted out or not report requested adult immunizations to the NDIIS.

2. Patient Consent Not Required

Written consent is not required prior to immunization information being entered into the NDIIS. This is in accordance with the North Dakota Century Code 23-01-05.3.

3. Release of Information

North Dakota Code (23-01-05.3) permits health care providers, elementary or secondary schools, early childhood facilities, public or private postsecondary educational institutions, city or county boards of health, district health units and the state health officer to exchange certain immunization data. The immunization data that may be exchanged "is limited to the date and type of immunization administered to a patient and may be exchanged regardless of the date of the immunization."

SECTION II: USE OF THE DATA AND CLASSIFICATION OF THE USERS

Only authorized users will have access to the information in NDIIS and will use it only for authorized purposes. Health care providers, schools, childcare centers and statutorily-identified publicly funded programs can apply to participate in the system. A representative of each authorized organizational participant must sign a Provider Site Agreement and abide by its requirements. Each Provider Site will identify a Site Administrator, who will be responsible for authorizing individual users at the Provider Site. No user will be authorized to access the NDIIS without first signing a statement that they will comply with this Confidentiality Policy. Participation in the system is not required to coordinate or to report immunizations.

NDIIS users may access identifiable patient information in the system only as required to assure adequate immunization of a patient, to avoid unnecessary immunizations, to confirm compliance with mandatory immunization requirements, to control disease outbreaks, to print Certificates of Immunization, to report and to review vaccine exemptions and to notify patients (or parents of minor children) that they are due or past due to receive recommended immunizations.
NDIIS users may not:

- Reveal or share any records or immunization data except as necessary in the course of their official duties, unless they have proper authorization from the patient whose records or data will be shared.
- Examine or read any records or immunization data regarding family, friends, public figures, etc. except on a "need to know" basis.
- Discuss or reveal the content of records or the immunization data with any person unless both persons have the authority and a need 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 NDIIS except as needed to complete assigned tasks and duties.
- Contact a person whose contact information you obtain from an immunization record in the NDIIS, except on official business or in the course of official duties, without proper authorization from the NDIIS or without proper authorization from the individual to whom the information pertains.
- Engage in any conduct involving the NDIIS that would constitute a criminal offense or give rise to civil liability.

Providers, including health care personnel and public health personnel, are the NDIIS primary users. Providers agree to use NDIIS only for the immunization needs of its patients or the targeted population in a clinic's catchment area. Providers and their personnel may access the registry system only when needed to coordinate immunization services.

Schools and childcare centers are the secondary users of NDIIS. They are allowed read-only access for the age group that they serve.

Patients and/or parents/guardians may receive a copy of their own or their child's immunization record from their own health care provider if the provider participates in NDIIS or from their local public health unit. Authorized health care providers and local public health units must allow the parent or guardian to inspect, copy, and if necessary, amend or correct their own child's immunization record if he/she demonstrates that record is incorrect by a credible source. A credible source is defined as a written immunization record from a healthcare provider or another immunization information system. An oral history of immunizations is not acceptable.

SECTION III: DATA ACCESS AND SECURITY PROCEDURE

Each user is responsible for maintaining the confidentiality of information contained in NDIIS. Each user is required to electronically sign a NDIIS confidentiality agreement annually.
Security Procedures

1. All users must safeguard his/her user ID and password.
    - Do not give a user ID and password to others.
    - Do not post a user ID and password.
    - Change password periodically, at least every 90 days

2. The NDIIS program must maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of health information.
    - The NDIIS central database resides in a secured area.
    - NDDoH must establish the firewall protection of its computing network to prevent access by unauthorized individuals.
    - NDIIS must use data encryption technology in its internet application.
    - NDIIS must provide periodic training on privacy and data security to its staff and users.

- NDIIS must conduct periodic assessments on the implementation of its privacy and security policies.

NDIIS information is confidential and can only be used for those purposes outlined in this document. Violation of this policy will be followed by an investigation and appropriate legal action stipulated in ND Century Code 23-01.3-09, which includes a penalty for unauthorized disclosure of health information. NDIIS privileges can be revoked pending results of the investigation.

3. The NDIIS does not delete client information. All information is retained within the NDIIS database.

User agreements are electronically renewed annually through the NDIIS. An electronic confirmation on the User Agreement Acknowledgement indicates that a user has read this policy, understands the content, and agrees to abide by its terms. A copy of this confidentiality policy is available at www.ndhealth.gov/immunize/ndiis and in the NDIIS Help Menu. The site administrator or authorized representative is required to notify the NDDoH as soon as possible – but no later than one week after - when any user account that requires termination due to an employee resignation or change in job responsibilities that no longer require access to NDIIS.

4. Users must comply with North Dakota Century Code Chapter 51-30, which outlines the procedures for reporting a security breach of personal information.

North Dakota Century Code 51-30-02 requires that "any person that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition, any person that experiences a breach of the security system as provided in this section shall disclose to the attorney general by mail or email any breach of the security system which exceeds two hundred fifty individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system."

North Dakota Century Code 51-30-05 requires that "notice under this chapter may be provided by one of the following methods:

1. Written notice;
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; or
3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice consists of the following:
    a. E-mail notice when the person has an e-mail address for the subject persons;

b. Conspicuous posting of the notice on the person's website page, if the person maintains one; and
c. Notification to major statewide media."

As a user of the NDIIS, I acknowledge that I have read and understand this policy and agree to the terms and conditions of this policy.

Figure 11. Memorandum of Understanding Sample (from North Dakota IIS)

MEMORANDUM OF UNDERSTANDING

This is an agreement between the state of North Dakota acting through its Department of Health ("State"), and the _____("Provider"). Each of the State and _____ is sometimes referred in this Agreement as "Party" and both are sometimes referred in this Agreement together as "Parties."

Whereas, the North Dakota Department of Health has established and maintains a statewide registry of immunization data, the North Dakota Immunization Information System ("NDIIS") pursuant to N.D.C.C. § 23-01-05.3;

Whereas, the North Dakota Department of Health contracts with Blue Cross Blue Shield of North Dakota to maintain NDIIS;

Whereas, health care providers are required to submit immunization data to NDIIS;

Whereas, NDIIS data is Protected Health Information subject to protection under the HIPAA Rules, as amended;

Whereas, NDIIS data is accessed and disclosed in a manner consistent with state law and the HIPAA Rules;

Whereas, the North Dakota Department of Health has engaged with Blue Cross and Blue Shield of North Dakota and immunization providers to create bi-directional interoperability between the provider electronic medical record and NDIIS;

Whereas, the Provider has agreed to connect the Provider electronic health record system to NDIIS, whether directly or through third party software, and will be provided with a single security credential allowing bi-directional access to the test and production systems and databases. During the project testing phase of work, this access will allow project team members to connect and test interoperability with the NDIIS. Post project, the single security credential will allow bi-directional access to the production system and database for use by approved provider practice employees and access to the test system and database for ongoing maintenance, support, and testing;

Whereas, the parties agree to comply with the terms and conditions of this Agreement and to comply with the storage, use and disclosure of Protected Health Information under the HIPAA Rules, all as amended from time to time;

Now therefore, in consideration of the mutual promises set forth in this Agreement, the Parties agree as follows.

SECTION 1. DEFINITIONS

Catch-all definitions:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Business Associate, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Protected Health Information "PHI"), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

a. Authorized User. "Authorized User" means an individual who is authorized by a Provider to access, use or disclose Protected Health Information in NDIIS and includes health care practitioners, employees, contractors, agents, or business associates of a Provider.

b. HIPAA Rules. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

c. Provider. "Provider" means the means any person who delivers, administers, or supervises health care products or services, for profit or otherwise, in the ordinary course of business or professional practice and includes its Authorized Users.

SECTION 2. OBLIGATIONS AND ACTIVITIES OF PROVIDER

Provider agrees to:

a. not use or further disclose NDIIS data other than as permitted or required by this Agreement or as required by law;

b. require all Authorized Users to sign a confidentiality agreement before access to NDIIS is granted by the Provider. The confidentiality agreement must include the following:

   i. statement of permitted use of data;

   ii. statement of prohibited use and disclosure of data;

   iii. agreement to comply with Provider's policies, procedures, and HIPAA Rules;

   iv. agreement to maintain NDIIS information confidential;

   v. agreement to comply with security provisions and password protections; and

   vi. sanctions or consequences of non-compliance.

c. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement;

d. comply with any limitation on the use or disclosure of a specified individual's PHI, if the State has notified the Provider of the limitation;

e. mitigate, to the extent practicable, any harmful effect that is known to the Provider or of a use or disclosure of PHI by the Provider or its Authorized Users in violation of the requirements of this Agreement;

f. in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that Business Associates and their subcontractors that create, receive, maintain, or transmit PHI received from NDIIS on behalf of the Provider agree to the same

restrictions, conditions, and requirements that apply to the Provider with respect to that information;

g. report to State any use or disclosure of the PHI not provided for by this Agreement of which the Provider becomes aware without unreasonable delay and in any case within 30 days from the date Provider becomes aware of any such unauthorized use or disclosure, including breaches of Unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which Provider becomes aware;

h. in the event of a the discovery of a Breach of Unsecured PHI, Provider shall provide the State with a written notification that complies with 45 C.F.R. § 164.410 which shall include the following information:

    i. to the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Provider to have been, accessed, acquired or disclosed during the breach;

    ii. the date of discovery of the breach and date of the breach;

    iii. the nature of the PHI that was involved;

    iv. identity of any person who received the non-permitted PHI;

    v. any steps individuals should take to protect themselves from potential harm resulting from the breach;

    vi. a brief description of what the Provider is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

    vii. any other available information that a Provider is required to include in notification to an individual under 45 C.F.R.§ 164.404(c) at the time of the notification to the State required by this subsection or promptly thereafter as information becomes available.

i. with respect to any use or disclosure of Unsecured PHI not permitted by the Privacy Rules that is caused by the Provider's failure to comply with one or more of its obligations under this Agreement, Provider agrees to pay its reasonable share of cost-based fees associated with activities State must undertake to meet its notification obligations under the HIPAA Rules and any other security breach notification laws;

j. make any amendment(s) to PHI in a designated record set as directed or agreed to by the State pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy the State's obligations under 45 C.F.R. § 164.526 within thirty (30) days after receiving a written request from the State;

k. make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules;

l. maintain and make available the information required to provide an accounting of disclosures to the State, within thirty (30) days after receiving a written request from

State, as necessary to permit the State to satisfy its obligations under 45 C.F.R. § 164.528;

m. without unreasonable delay, report to State any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system of which the Provider becomes aware of in accordance with 45 C.F.R. § 164.314(a)(2)(C); and

n. monitor and conduct audits of access to and use of NDIIS by its authorized users.

SECTION 3. PERMITTED USES AND DISCLOSURES BY PROVIDER

a. Regulatory Duties

Provider acknowledges that it has a duty to comply with the HIPAA Rules and further acknowledges that its failure to comply with any applicable HIPAA Rules could result in civil or criminal penalties under 42 U.S.C. §§ 1320d-5 and 1320d-6.

b. General Use and Disclosure Provisions.

1. Except as otherwise limited in this Agreement, Provider may use or disclose PHI to perform its functions, activities, or services, as or as required by law.

2. Provider agrees to make uses, disclosures and requests for PHI consistent with the minimum necessary amount of information needed to perform the activities permitted in this agreement.

3. Provider may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the State or a Covered Entity, except that unless otherwise limited in this Agreement.

4. Except as otherwise limited in this Agreement, Provider may disclose PHI to a Business Associate for the proper management and administration of the Provider, provided the disclosure is required by law or Business Associate complies with the applicable requirements of the HIPAA Rules.

5. Provider may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

6. Provider may not receive direct or indirect remuneration in exchange for PHI except as permitted by the HIPAA Rules.

SECTION 4. OBLIGATIONS OF STATE

The State shall:

a. notify Provider of any changes in, or revocation of, permission by an Individual to use or disclose his or her PHI, to the extent that any such changes may affect Provider's use or disclosure of PHI;

b. notify Provider of any restriction on the use or disclosure of PHI that State has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that the restriction may affect Provider's use or disclosure of PHI.

c. obtain any consent or authorization that may be required by applicable federal or state laws and regulations prior to furnishing PHI to the Provider; and

d. not request Provider to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by State, except that the Provider may use or disclose PHI for data aggregation or management and administration and legal responsibilities of the Provider.

SECTION 5. TERM AND TERMINATION

a. Term. The Term of this Agreement shall be effective upon execution, and shall terminate upon a thirty (30) day written notice of termination by either Party. Upon termination, all PHI provided by State to the Provider or received by Provider to the State, shall either be destroyed, returned to State or, if it is not feasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this section.

b. Termination for Cause. Upon the non-breaching Party's knowledge of a material breach by the other Party (the "breaching party"), the non-breaching party shall either:

1. provide an opportunity for the breaching party to cure the breach or end the violation within thirty (30) days and terminate this Agreement if the non-breaching party does not cure the breach or end the violation within the thirty (30) day period;

2. immediately terminate this Agreement if the breaching party has breached a material term of this Agreement and cure is not possible; or

3. if neither termination nor cure is feasible, report the violation to the Secretary.

c. Obligations of Provider upon termination.
Upon termination of this Agreement for any reason, Provider, with respect to PHI received from State, or created, maintained, or received by the Provider to the State, shall:

1. retain only that PHI which is necessary for Provider to continue its proper management and administration or to carry out its legal responsibilities; and

    a. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as the Provider retains the PHI;
    b. not use or disclose PHI retained by Provider other than for the purposes for which the PHI was retained and subject to the same conditions set out in this Agreement; and

2. return to the State or, if agreed to by the State, destroy the remaining PHI that the Provider maintains in any form; or

3. return to the State or, if agreed to by the State, destroy the PHI retained by any contractor or subcontractor when it is no longer needed for its proper management and administration or to carry out its legal responsibilities.

d. Survival. The obligations of the Provider under this Section shall survive the termination of this Agreement.

SECTION 7. MISCELLANEOUS

a. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as may be amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

c. Indemnification. Provider shall indemnify, defend, and hold State and its employees, directors, trustees, officers, representatives and agents (collectively the Indemnitees) harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys' fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of any material breach of the terms of this Agreement by Provider.

d. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

The parties have caused this Agreement to be executed on the date signed below.

PROVIDER:_____

BY: _____

ITS: _____

DATE: _____

STATE OF NORTH DAKOTA, acting through its Department of Health

BY: _____

ITS: _____

DATE: _____

Figure 12. User/Usage Agreement Sample (from Michigan IIS)

MICHIGAN CARE IMPROVEMENT REGISTRY
POLICY AND PROCEDURES

Number: 01-02 v.3	**Subject:** MCIR User/Usage Agreement Processing
Effective Date: 06-15-07	**Authority:** MDCH, Regional Staff
Date Approved: 06-15-07	**Page:** 1 of 2

Policy Statement: Regional MCIR offices are responsible for verification and processing of provider user/usage agreements. All activities associated with processing of these agreements shall be conducted in a timely, efficient, effective and professional manner. Confidentiality, accuracy and accountability will be maintained at all times.

Purpose of Policy:

This policy shall establish uniform standardized procedures to ensure that:

- User/usage agreements are processed in a uniform and timely manner;
- Requests to access the MCIR are timely verified, processed and approved;
- The licensure status of Michigan health care providers is accurately assessed; and
- Proper credentialing of other organizations is conducted.

Responsibility:
The MCIR Regional coordinator and assigned staff shall ensure that:

- User/usage agreements are processed in a timely manner.
- All information pertaining to a user/usage agreement is maintained in manner ensuring the confidentiality and integrity of provided documentation.

Procedure: The procedure set forth below establishes standards for the distribution, receipt, processing, and approval/denial of MCIR user/ usage agreements. This includes verification and validation of the requesting organization and/or the health care provider. Regional MCIR Administrator rights will be issued by the Michigan Department of Community Health (MDCH).

A. Distribution of User/Usage Agreements may occur with or without a MCIR information/training packet. If an information training packet is provided, it is recommended that the following be included:
    1. Instructions for completing a MCIR user/usage agreement;
    2. MCIR Reporting (Opt Out) form;
    3. Petition for Modification to MCIR Information form including instructions;
    4. Registry information pamphlet;
    5. Name and phone number of the Regional MCIR Coordinator; and
    6. Any other relevant materials.

B. MCIR user/usage agreements may be distributed in the following manner:
    1. Through regional MCIR outreach efforts including presentations;
    2. Through local health departments and their IAP Coordinator
    3. Through MDCH Regional Field Representatives;
    4. MDCH, Division of Immunization;
    5. Downloaded from the Resource Library at www.mcir.org; and
    6. Directly from the Regional MCIR office upon request.

C. Processing of MCIR user/usage agreements:
    1. Thoroughly completed agreements will be submitted to the Regional MCIR office;
    2. Upon receipt, agreements will be timely reviewed and processed;

12

3. New sites will be timely added to the MCIR and issued a site ID;
4. Identified designated users will be attached to the MCIR Site ID and provided with instructions for MCIR User Registration;
5. New users will be counseled regarding sharing of MCIR login information constitutes a breach of HIPAA standards as well as the MCIR User/Usage Agreement;
6. If a provider site fails to timely submit a completed MCIR User Agreement (renewal) the Regional MCIR office may at its discretion terminate MCIR access rights to the provider until such time as signed updated agreement is received. A determination to discontinue access rights to the MCIR shall be made on a case by case basis following a thorough review of all pertinent information.

D. Verification of Provider/Organization License:
    1. Health care Provider licensure is verified:
        a. Online through MDCH: http://www.dleg.state.mi.us/free/default.asp; and
        b. Through proof of current licensure status submitted by the provider;

Verification of other non-provider organizations may be conducted by contacting the organization's CEO, director, president or administrator. Under certain circumstances a certifying or licensing agency may be available.

E. Non-Verification of Provider/Organization:
    1. If a health care provider or organization cannot be verified, the provider/organization shall be notified in a timely manner:
    2. The health care provider or organization is then responsible for further investigation and resolution of the underlying circumstances resulting in non-verification; and
    3. It is the responsibility of the health care provider or organization to contact the Regional MCIR Office to provide additional information allowing for resolution of the non-verification.

F. Retention and filing of User/Usage Agreements
    1. Completed, verified and processed user/usage agreements will be retained on file at the Regional MCIR Office; and
    2. User/Usage Agreements will be appropriately stored and maintained to maintain confidentiality and document integrity.

G. Requests for User IDs and Passwords:

When the Regional MCIR office is contacted regarding forgotten User IDs or passwords. The password will not be reset until the Regional office validates that the provided information (user, site) is appropriate to the request.

H. Revocation of Password and I.D. numbers:
    1. The revocation of a MCIR Site ID or of a user's login and password may be necessary under circumstances in which the confidentiality of an ID has been compromised or when the provider who signed the user/usage agreement departs from employment with the organization;
    2. 2. It is the responsibility of the Regional MCIR office to proceed with the revocation process or in the alternative with processing of a new MCIR user/usage agreement as appropriate;
    3. Organizations and users active in the MCIR will be notified of the termination of their rights and rationale(s) surrounding the termination; and

4. The organization will be notified by the Regional MCIR office of the need to prepare and submit a new MCIR user/usage agreement if appropriate.

I. MCIR Registration Renewal

MCIR User/Usage Agreements are valid for a period of three (3) years from the date of signature. A new form shall be prepared, signed and submitted by the provider/organization to ensure continued, uninterrupted MCIR access. It should be noted that processing of MCIR User/Usage Agreement renewals are subject to the licensure verification process.

Related Policies and Procedures: None

Note: Comparable to MDCH Policy 01-01 v.2

Revision and Review History: Reviewed 6-15-07, 10-23-13; Revised 10-14-2011

Adopted: 6-16-2005

Figure 13. Confidentiality Guidelines Sample (from Michigan IIS)

MICHIGAN CARE IMPROVEMENT REGISTRY
POLICY AND PROCEDURES

Number: 01-01 v.1	**Subject:** MDCH/MCIR Confidentiality Guidelines
Effective Date: 06-15-07	**Authority:** MDCH, Regional Staff
Date Approved: 06-15-07	**Page:** 3 of 6

Policy Statement: Each Regional Office of the Michigan Care Improvement Registry (MCIR) will be responsible for the Confidentiality of information pertaining to the information gathered and held within. Using these guidelines, Regional staff will ensure that confidentiality, accuracy, timeliness, and accountability will be of the highest standards.

Purpose of Policy: To ensure that there is a standard procedure in place for maintaining confidentiality throughout all Regional activities.

Responsibility: It is the responsibility of all Regional Staff to safeguard the confidentiality of the information flowing in and out of the registry.

Procedure: The following guidelines, compiled by the Michigan Department of Community Health, outline the procedures for maintaining confidentiality and addressing security issues should they arise.

Confidentiality Guidelines for
The Michigan Care Improvement Registry (MCIR)

Notice: These guidelines, any part or its entirety, are subject to revisions by the Michigan Department of Community Health (MDCH) at any time without advanced notice provided to all interested agencies and/or providers.

I. Introduction

In 1996, the 88th Legislature of the state of Michigan passed Public Act 540 (PA 540) Section 9207 of the act sanctioned the Michigan Department of Community Health the right to establish an immunization registry, to be known as the Michigan childhood immunization registry, to record information regarding immunizations performed by immunization providers. Subsection (2) of Section 9207 states *The information contained in the childhood immunization registry is subject to the confidentiality and disclosure requirements of this section and sections 2637 and 2888 and to the rules promulgated under section 9227* (see those sections for additional information). Thus PA 540 requires that information contained in the MCIR be kept confidential. In 2006, the legislature of the State of Michigan adopted section 333.9207 Childhood immunization registry; Michigan care improvement registry; establishment; purpose; confidentiality and disclosure requirements Sec. 9207:
(1) The department shall establish a registry, to be known as the "childhood immunization registry", to record information regarding immunizations performed under this part. Beginning after the effective date of the amendatory act that added section 9227(2), the "childhood

immunization registry" shall be known as the "**Michigan Care Improvement Registry**". The department shall enter information received under sections 2821 and 9206 in the registry.
(2) The information contained in the registry is subject to the confidentiality and disclosure requirements of sections 2637 and 2888 and to the rules promulgated under section 9227. The department may access the information contained in the registry when necessary to fulfill its duties under this code.
(3) Upon receipt of a written request from an individual who is 20 years of age or older, the department shall make any immunization information in the registry pertaining to that individual inaccessible. The written request shall be in a form prescribed or otherwise authorized by the department**.** The administrative rules for section 333.9227:

(1) The department shall promulgate rules to implement this part, including, but not limited to, rules governing all of the following:

(a) Age periods for immunizations.
(b) The minimum ages at which immunization may be commenced.
(c) The minimum number of doses required during a specified time period.
(d) Minimum levels of immunization for children in school.
(e) Reporting under section 9206(3).
(f) The acquisition, maintenance, and dissemination of information contained in the registry established under section 9207.

(2) The department shall promulgate rules to implement the expansion of the registry to include the reporting and recording of additional information such as lead screening performed on children**.**

The confidentiality policy is intended to delineate and ensure this firm level of confidentiality. This document addresses the following information:

Section	Description
Section II	Describes the levels of access granted to various immunization providers, states the MCIR usage agreement policy, and outlines the penalties in place for violating the confidential policy.
Section III	Indicates how parents and individuals are notified of the registry
Section IV	Provides information on how parents and individuals may choose to not participate in the MCIR.
Section V	Describes the purposes of collecting the immunization information, and how the information will be used.
Section VI	Provides information on the varying degrees of access to the registry by different providers is delineated in section.
Section VII	Outlines the penalties for inappropriate use or disclosure of immunization information.

II. Agreements to Protect Confidentiality

Access to the MCIR is permitted for the sole purpose of providing information and documentation needed for immunization purposes. This access is permitted under the provisions of MCL 540.9201, 9206, and 9227. Access to MCIR data is under the terms and conditions prescribed the MDCH, and stipulated below.

Users, defined as anyone with access to the MCIR, must register and sign a formal user/usage agreement Users are categorized into one of the following user types:

1 Public Provider
2 Private Provider
- Family Practice
- Pediatrician
- Internist
- OBGYN
- Site Administrator
- Pharmacies
- Long Term Care

3 School/Daycare/Camp Site Administrators
4 Health Care Organizations
5 WIC
6 Health Department Administrative Staff
7 MDCH Authorized Agent
8 MCIR Regional Administrators

Providers, defined as those who can authorize the administration of any immunizing agent (as defined by Public Health Code MCL 333 9204), can be registered individually, or by organization. In the latter case, the organization assumes full responsibility and liability for the individual's usage of the MCIR, including any penalties associated with improper usage of the MCIR and/or any immunization data associated with the MCIR.

Any physicians who practice outside of the state of Michigan but regularly treat residents of Michigan (i.e., areas bordering Michigan) may be registered as MCIR users. Such providers need to enter demographic and immunization encounter data for their patients who are Michigan residents. The MCIR will not contain restrictions on entering data for children with out-of-state addresses.

Different user types will have varying degrees of access to MCIR data (see below). Anyone wishing to use the MCIR must first register with the MCIR as a user by reading and signing a user/usage agreement.

All registered sites in MCIR have a Site Administrator responsible for adding or removing additional users for each site. This individual is responsible for adding new users as well as invalidating users to their site in the MCIR.

The first step to receive access to the Michigan Care Improvement Registry:

1. A site must designate a Site Administrator and complete a Provider Usage Agreement. This agreement is then sent to the MCIR Regional Office for processing. The MCIR staff registers the site in MCIR, and then trains the site administrator on the user registration process.

2. Once the Site Administrator completes the registration process, they have the ability to add other MCIR users to their site.

3. When a site administrator enrolls a user to the system the user receives a pin number through an email from mcir@michigan.gov

4. The user logins to the Single Sign Portal and creates a user id that includes The User ID will be the user's last name & first initial plus the 4-digit number that they enter.

5. Single Sign On system requires users to answer and confirm a set of Challenge/Response Questions

6. The user will then subscribe to MCIR with the PIN number through the SSO application.

7. Users are required to change their password and answer the challenge/response questions

8. Registered users are required to change your password every 90 days.

9. Every year a register user is required to accept the MCIR User/Usage Confidentiality Agreement online.

In addition, regional coordinators and/or staff are responsible for re-verifying or re-certifying provider licenses or organizations every three years. The following process outlines an acceptable method for re-verification or re-certification of provider licenses or organizational status to ensure that users of the MCIR are appropriately licensed providers or organizations in Michigan.

Every three years the provider licenses will be re-verified and every three years an organization or individual within the organization will be re-certified.

Provider licenses are re-verified as follows:

A. Primary verification method is to use the Michigan Department of Licensing and Regulatory Affairs

B. If a provider license cannot be verified, the provider will be personally notified within one business day. The provider's User ID/password will then be immediately inactivated within one business day.

C. If a provider license cannot be re-verified, the provider will be personally notified, within one business day. The provider's User ID/password will then be inactivated within one business day.

D. It will be the provider's responsibility to investigate the issues related to the non-verification.

Organizational status will be re-certified as follows:

A. Primary re-certification method is to use the licensing agency, the parents organization (e.g., school district office for a school).

B. To re-certify an individual in a school district, such as the principal of a school who signed the MCIR School User/Usage Agreement, the school district office can be contacted.

C. If an organization or an individual within the organization cannot be re-certified for any reason, the organization and/or individual will be notified personally within one business day. The organization or individual Password and User ID will then in inactivated within one business day.

D. It will be the responsibility of the organization or individual to investigate the issues related to non-verification.

As a registered user of the MCIR, users agree to the following stipulations:

- Users will handle information or documents obtained through the MCIR in a confidential manner.
- Users will restrict their use of the MCIR to accessing information and generating documentation only as necessary to properly conduct the administration and management of their duties as they relate to immunizations.
- Users understand that transactions on the MCIR are logged and are subject for review for overall usage.
- Users will not furnish information of documentation obtained through the MCIR to individuals for personal use nor to any individuals not directly involved with the conduct of the duties of the user as they related to the administration, recording, and reviewing

immunizations.

- Users will not falsify any document or data obtained through the MCIR.
- Users will not attempt to or copy all or any part of the database or the software used to access the MCIR database for any unapproved purpose, nor attempt to falsify or otherwise alter data in the MCIR database, or otherwise violate all or any portion of the Michigan Computer Crime Law (MCL 333.791-333.797) or the Vital Records Law (MCL 333.2894) summarized on the back of the user/usage agreement.
- Users will carefully and deliberately safeguard their access privileges and password for the MCIR and will not permit the user of such access privileges by any other person, unless expressively authorized by MDCH to possess such use.
- Users agree to reports any threat to or violations of (whether real or perceived) to the appropriate MCIR security personnel.

Any improper use of the MCIR that violates the preceding stipulations will result in revocation of the user's access privileges and may include official penalties and/or sanctions as specified in Public Act 540 of the Public Acts of 1996 (see attachment A), the Vital Records Law (MCL 333.2898), or the Michigan Computer Crime Law (Sec 752.797).

III. Notification

Pursuant to Section 2828 (3) of Public Act 540, upon receipt of a vital record consisting of a birth registration transmitted by a local registrar pursuant to section 2815(2), the state registrar shall transmit the information contained in the birth registration to the childhood immunization registry created in section 9207. Thus, state laws do not require that parents receive any verbal and/or written notification that their child's immunization records will be loaded into and become part of the MCIR database. All Vaccine Information Statements (VIS) provided by the MDCH contain a paragraph informing parents that all immunizations administered to their children will be entered into the MCIR unless the parent signs an opt-out form. All parents of children born in a Michigan hospital should receive a Child Passport. Included in this package will be information about the MCIR

IV. Participation

The MCIR was authorized by the legislature to permit parents to opt-out if they so choose. Parents/individuals who do not want immunization information about themselves or their children in the MCIR are required to sign an opt-out form, which may be obtained from the local health department, immunization provider or the Regional Immunization Coordinator.

Immunization and demographic information on any person who has chosen to opt-out is then no longer accessible by users and no reminder or recalls are generated. However, a persons basic demographic information - date of birth, gender and name remain within the MCIR for purposes of accurately determining the population for the sole purpose of calculating community and state immunization rates.

Parents/individuals may choose not to receive Reminder/Recall notices. If a parents/individuals chooses not to receive these notices they may notify their immunization provider to document this in MCIR.

V. Use of Immunization Registry Data

MCIR benefits health care organizations, schools, licensed childcare programs, and Michigan's citizens by consolidating immunization information from multiple providers. This reduces vaccine-preventable diseases, over-vaccination, and allows providers to see up-to-date patient immunization history. MCIR is governed by P.A.368 333.9207
and the associated rules R 325.162. MCIR assists providers in keeping a persons immunization status up-to-date, decreases the number of duplicate vaccines administered, and gives the provider an efficient means by which to track a persons immunization history. More succinctly, the MCIR:

- Maintains immunization histories through the lifespan for individuals.
- Gives providers and other interested parties the ability to quickly and efficiently look up a person's immunization status.
- Provides a report of immunizations that are due.
- Evaluates immunization status and recommends future dose dates.
- Gives interested parties the ability to enter immunization information into the MCIR via the web-based user interface or through electronic messaging.
- Provides immunization assessments.
- Can assess immunization coverage of a population.
- Assists in streamlining vaccination reports.
- Provides different levels of data access (see below), and safeguards confidentiality.
- Allows a provider to manage their vaccine inventory.

VI. Access to and disclosure of Information

Access to the MCIR is restricted to Immunization Providers and others, such as schools and day care centers who have a need for such access, as well as technical and program staff at local and state health departments and the MCIR Regional Administrator. The following table outlines the different types of access to MCIR data that are allowed for each user group (type). Note that "Add Person" means that the provider has the ability to add a person demographic record into the MCIR database. "Update Person Info" means the provider has the authority to alter demographic information already appearing as part of a specific record; "Add Immunization Encounter" grants the provider access to add immunization information to a persons record; "Modify Immunization Encounter" means that the provider can change immunization data they entered into the MCIR; "View Immunization Status" allows providers to assess the if a person is up-to-date, not up-to-date, or overdue with respect to their immunization status; and "View Immunization History" gives providers permission to examine the entire immunization history (immunization record) of a person in MCIR.

User Type	Add Person	Update Person	Add Immunization Encounter	Modify Immunization Encounter	View Immunization Status	View Immunization History
Providers (public and private)	*	*	*	*	*	*
Health care organizations					*	*
Schools/day cares/camps	*	*	*	*	*	*
Health Department Administrator					*	*
MDCH authorized agents	*	*	*	*	*	*
MCIR Regional Administrator	*	*	*	*	*	*
WIC					*	*

* = Has authorization.

Users are classified and provided a discrete level of access based on the information they need to obtain in order to carry out specific functions. That is, access is granted to users only on a need-to-know basis. Providers have a limited browse (10 records) from the MCIR database, and must enter unique identifying demographic information into the MCIR to locate a persons record. In addition, providers can only enter additional information into the MCIR, and can only alter information they specifically entered. If a provider finds that information entered by another agency or provider is incorrect, the provider who finds the error must complete a petition for

modification form that indicates what error(s) was made, requesting that it be corrected by their regional coordinator.

All authorized users must sign a User Agreement before they are provided with a unique username and password from the State of Michigan's Single Sign On Application to access the MCIR.

All requests for research use of the data should be directed to the Immunization Division and the Internal Review Board at the Michigan Department of Community Health. The request will be reviewed by the State Internal Review Board and approved, refused or returned for additional information.

Disclosure of MCIR data on individuals by users to others, including law enforcement is specifically prohibited. All sub-pœnas and other legal demands for MCIR data received by any authorized user of the MCIR should be referred to the Division of Immunization, Michigan Department of Community Health. Responses to these matters will be in accordance with MDCH policy on sub-pœnas, court orders and other legal documents by the Office of Legal Affairs.

VII. Penalties for Unauthorized Disclosures

The Division of Immunizations has controls in place that when a person reports a misuse of MCIR data the MCIR technical staff may review the audit logs to research a breach of confidentiality. The user name, time stamp and access to records are recorded in the audit file. All users are required to follow HIPAA guidelines with printed and electronic information in their medical offices. Schools are required to follow Family Education Rights and Privacy Act (FERPA) guidelines for protect student information.

As previously indicated in Section II of this policy, any breach or violation of any portion of the stipulations delineated in the User/Usage Agreement that the user signs will result in revocation of the user's access privileges and may include official penalties and/or sanctions as specified in Public Act 540 of the Public Acts of 1996 (see attachment A), the Vital Records Law (MCL 333.2898), or the Michigan Computer Crime Law (Sec. 752.797). Please see the appropriate statute for the specific penalties associated with violation of a particular mandate. For example, a person who is found to be in violation of the Vital Records Law is guilty of a misdemeanor punishable by imprisonment for not more than 1 year, or a fine of not more than $1,000.00, or both. A departmental employee who violates this regulation shall be subject to immediate dismissal.

Amendment: November 2013

Figure 14. Record Request and Release Form Sample (from Michigan IIS)

MICHIGAN CARE IMPROVEMENT REGISTRY
POLICY AND PROCEDURES

Number: 01-06 v.2	**Subject:** MCIR Record Requests and Releases
Effective Date: 06-15-07	**Authority:** MDCH, Regional MCIR Staff, all MCIR Users
Date Approved: 06-15-07	**Page:** 1 of 1

Policy Statement: Immunization information maintained in the MCIR constitutes the official immunization record for the State of Michigan. Immunization data maintained in the MCIR is proprietary to the State of Michigan. The Michigan Department of Community Health (MDCH) retains responsibility for processing requests for release of MCIR information. However, MDCH specifically authorizes Regional MCIR offices to release MCIR information under circumstances in which there is no indication that the requested information will be utilized in a legal proceeding. In complying with a parent or an individual's request for MCIR data, Regional MCIR offices shall utilize the form entitled *Request for Official State of Michigan Immunization Record*.

Purpose of Policy: To identify the procedure for releasing an Official State of Michigan Immunization Record from MCIR to the individual(s) listed as Responsible Party in MCIR, referring requests submitted to Region 1 MCIR via subpoena, freedom of information act (FOIA), court order or other legal demand by attorneys, law firms, health care organizations, law enforcement, etc. to MDCH for review and further processing as appropriate.

Responsibility: Region 1 MCIR staff and users are responsible for ensuring that MCIR records are only released to the appropriate parties:
1. Any Responsible Party indicated in the MCIR
2. Other medical practices, schools or Health Care Organizations for immunization assessment purposes only.

Pursuant to MDCH MCIR Confidentiality Guidelines – Disclosure of MCIR data on individuals by users to others, including law enforcement is specifically prohibited. All subpoenas and other legal demands for MCIR data received by any authorized user of the MCIR should be referred to the Division of Immunization, Michigan Department of Community Health. Requests will be responded to in accordance with MDCH policy on subpoenas, court orders and other legal documents by the Office of Legal Affairs.

Procedure for all MCIR users:
1. All subpoenas, FOIA requests, court orders and any other legal demands for MCIR information shall be timely forwarded to the Michigan Department of Community Health, Division of Immunization, attention MCIR, PO Box 30195, Lansing, Michigan 48909.
2. Medical practices, schools, LHDs or other Health Care Organizations should follow their internal policies for records releases.
3. Records released should be the 1-page Official State of Michigan immunization record without address.

Procedure for Region 1 MCIR staff:
1. All individual requests for Official State of Michigan Immunization records should initially be referred to the individual's provider or local health department for release. Requests made via subpoena, freedom of information act (FOIA), court order or other legal demand by attorneys, law firms, health care organizations, law enforcement, etc. shall be referred to MDCH for review and further processing as appropriate.
2. If the individual's provider or LHD is unavailable or unable to process the request, individuals should be provided with the *Request for Official State of Michigan Immunization*

19

Record form to complete and send in along with a copy of the requestor's state issued identification card or driver's license.

3. Once the completed *Request for Official State of Michigan Immunization Record* form is received along with supporting documentation, Region 1 MCIR staff will process the request within 14 business days.

Related Policies and Procedures: #01-01 *MDCH/MCIR Confidentiality Guidelines*; *VFC & MI-VFC Provider Resource Book* (*II-pgs. 6&7)*.

Notes: For the "Penalties for Unauthorized Disclosures," see policy #01-01 *MDCH/MCIR Confidentiality Guidelines.*

Revision and Review History: Reviewed 6-15-07, 10-23-13; Revised 10-14-11

Adopted: 06-16-2005

Figure 15. Data Access Policy Sample (from Michigan IIS)

MICHIGAN CARE IMPROVEMENT REGISTRY
POLICY AND PROCEDURES

Number: 04-01	**Subject:** MCIR Data Access
Effective Date: 06-15-07	**Authority:** MDCH and Regional Staff
Date Approved: 06-15-07	**Page:** 1 of 1

Policy Statement: Region 1 MCIR will ensure that access to the registry and/or data will only be given to approved/licensed sites/users that have completed the necessary User Agreements and registration processes.

Purpose of Policy:
To assure only approved users are given access to the registry to protect the confidentiality/use of MCIR data.

Responsibility: All Regional MCIR Staff are responsible for safeguarding MCIR data, giving MCIR access only to registered sites/users.

Procedure:

1. Prior to issuing Site/User Ids and passwords for MCIR access, the region will have all of the appropriate signed documentation on file.
2. Individual site data will not be shared with other sites unless permission is granted from the Provider/Site Administrator, using the *Provider MCIR ID Usage Consent Form*.
3. Local health departments will be allowed to see more detailed data from VFC sites, as well as population coverage reports for all providers in their jurisdiction (per VFC agreement and accreditation language).
4. Any misuse of the MCIR will result in immediate suspension of MCIR access, with potential termination of access rights after further investigation.

Related Policies and Procedures: #01-01 *MDCH/MCIR Confidentiality Policy*; # 01-03 *Cancellation of MCIR Site, User ID and/or Password Information.*

Notes: None

Revision and Review History: Reviewed 6-15-07, 10-23-13; Revised 10-14-11

Adopted: 06-16-2005

http://www.immregistries.org

This document is published by American Immunization Registry Association (AIRA), an organization founded to advocate for the support of immunization information systems.