Minnesota Immunization Information Connection

Information Technology Audit

January 2023

Financial Audit Division

Office of the Legislative Auditor

State of Minnesota

50 YEAR ANNIVERSARY 1973 2023

Financial Audit Division

The division has authority to audit organizations and programs in the state's executive and judicial branches, metropolitan agencies, several "semi-state" organizations, state-funded higher education institutions, and state-funded programs operated by private organizations.

Each year, the division selects several of these organizations and programs to audit. The audits examine the policies and procedures—called internal controls—of the organizations to ensure they are safeguarding public resources and complying with laws that govern their financial and program operations. In addition, the division annually audits the State of Minnesota's financial statements and the financial statements of three state public pension systems. The primary objective of these financial audits is to assess whether the statements fairly present the organization's financial position according to Generally Accepted Accounting Principles.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division. The Program Evaluation Division's mission is to determine the degree to which state agencies and programs are accomplishing their goals and objectives and utilizing resources efficiently.

OLA also conducts special reviews in response to allegations and other concerns brought to the attention of the Legislative Auditor. The Legislative Auditor conducts a preliminary assessment in response to each request for a special review and decides what additional action will be taken by OLA.

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

OLA | OFFICE OF THE LEGISLATIVE AUDITOR

Judy Randall, Legislative Auditor
State of Minnesota

January 23, 2023

Members
Legislative Audit Commission

Members
Legislative Commission on Cybersecurity

Brooke Cunningham, Commissioner
Minnesota Department of Health

Tarek Tomes, Commissioner and Chief Information Officer
Minnesota IT Services

This report presents the results of our information technology performance audit of the Minnesota Immunization Information Connection, the state's immunization registry operated by the Minnesota Department of Health (MDH) and Minnesota Information Technology Services (MNIT). The objectives of this audit were to determine if MDH and MNIT had adequate internal controls to safeguard the confidentiality, integrity, and availability of the information system.

To reduce the security risk posed by Findings 2 and 5, we have removed language we deemed a security risk from this public version of our report. We discussed the specific details with MDH and MNIT.

This audit was conducted by Mark Mathison (IT Audit Director), Joe Sass (IT Audit Coordinator), and auditors Amanda Sayler and Peng Xiong.

We received the full cooperation of agency personnel while performing this audit.

Sincerely,

Lori Leysen, CPA
Deputy Legislative Auditor

Mark Mathison, CISA, CISSP, CPA (Inactive)
IT Audit Director

Room 140 Centennial Building, 658 Cedar Street, St. Paul, MN 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Website: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 711

OLA

Table of Contents

OLA

Introduction

The Minnesota Immunization Information Connection (MIIC) is an information technology system managed by the Minnesota Department of Health (MDH) and Minnesota Information Technology Services (MNIT). First launched in 2002, the system tracks and stores Minnesotans' immunization records and assists MDH in managing statewide immunization inventories. The system combines an individual's immunizations into a single record, even if the immunizations were given by different health care providers. Individuals who are born in or receive an immunization in Minnesota have a MIIC record.

MIIC contains information on nearly 127.5 million immunization doses administered to more than 9.5 million people. More than 16,000 user accounts—held by personnel in nearly 6,000 organizations (medical clinics, dental offices, pharmacies, schools, and child care facilities)—allow individuals to directly access the immunization records in MIIC. Due to the sensitive nature of immunization data and its importance in supporting Minnesota's response to disease outbreaks, MDH and MNIT must adequately control MIIC to ensure that the system and its data are accurate and protected from unauthorized use or disclosure.

We conducted this information technology performance audit to determine whether MDH and MNIT complied with applicable policies, standards, and best practices designed to protect the confidentiality, integrity, and availability of the MIIC system and its data. We audited system controls and agency processes related to access management, change management, data integrity, data privacy, disaster recovery, risk management, and system configuration.

OLA

Report Summary

Conclusion

The Minnesota Department of Health (MDH) and Minnesota Information Technology Services (MNIT) generally complied with applicable policies, standards, and best practices designed to protect the confidentiality, integrity, and availability of the Minnesota Immunization Information Connection (MIIC) system and its data. However, we found certain gaps in controls, some of which exposed the system to unnecessary risks.

Findings

Finding 1. MDH does not actively monitor whether users or participating organizations with access to MIIC comply with data use requirements. (p. 14)

Finding 2. MIIC does not meet all of the requirements defined within MNIT's logging and monitoring standard. (p. 15)

Finding 3. MIIC contains testing and training data in the production system. (p. 20)

Finding 4. MNIT did not use code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software. (p. 23)

Finding 5. MIIC contained exploitable vulnerabilities that could have allowed a compromise of user accounts and private data. (p. 24)

Finding 6. In the case of a disaster, MNIT may not meet expected system restoration timelines for MIIC due to an incomplete disaster recovery plan and architecture limitations. (p. 25)

Finding 7. MDH and MNIT did not complete a risk assessment on MIIC or use MNIT's central management tool, as required by MNIT's standards. (p. 27)

OLA

Background

Immunization Information Systems (IISs)

Immunization Information Systems (IISs), sometimes also known as immunization registries, are "confidential, population-based, computerized databases, that record all immunization doses administered by participating providers to persons residing within a given geopolitical area."[1] There are more than 60 independent IISs operating in the United States, including all 50 states and other territories or jurisdictions.[2] An IIS can provide a consolidated immunization history for an individual and assist medical providers in providing clinical care and determining what immunizations may be necessary. An IIS also provides aggregated data on immunizations for public health organizations, with the goal of improving immunization rates and reducing vaccine-preventable diseases. Exhibit 1 articulates how an IIS collects immunization data from a variety of sources and how individuals and authorized professionals can use the consolidated data.

IISs are governed and maintained at the state and local levels, with some variation in function, capacity, data quality, and regulations around sharing immunization information both within and outside of jurisdictions.[3] State laws authorizing operation of an IIS may 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.

While no federal laws prescribe requirements for an IIS, the Centers for Disease Control and Prevention (CDC)—in an effort to provide consistency among different systems—maintains a set of standards for IISs.[4] The Immunization Information System Functional Standards describe the operations, data quality, and technology needed by IISs to support immunization programs, vaccination providers, and other immunization stakeholders.[5] While not a federal requirement, these standards reflect the functionality an IIS should strive to attain to fully support program and stakeholder immunization-related goals.

In Minnesota, there are few laws related to its immunization information system and functions. Minnesota law requires the use of the state's IIS when vaccines are administered by pharmacies and dentists.[6] Outside of specific CDC requirements to report COVID-19

---

[1] Centers for Disease Control and Prevention, "About Immunization Information Systems," https://www.cdc.gov/vaccines/programs/iis/about.html, accessed November 17, 2022.

[2] A listing of all Immunization Information Systems can be found at https://www.cdc.gov/vaccines/programs/iis/contacts-locate-records.html, accessed January 3, 2023.

[3] Daniel W. Martin, Elaine N. Lowery, Bill Brand, et al., "Immunization Information Systems: A Decade of Progress in Law and Policy," *Journal of Public Health Management and Practice*, vol. 21, no. 3 (May 2015).

[4] The Centers for Disease Control and Prevention is based in the federal Department of Health and Human Services.

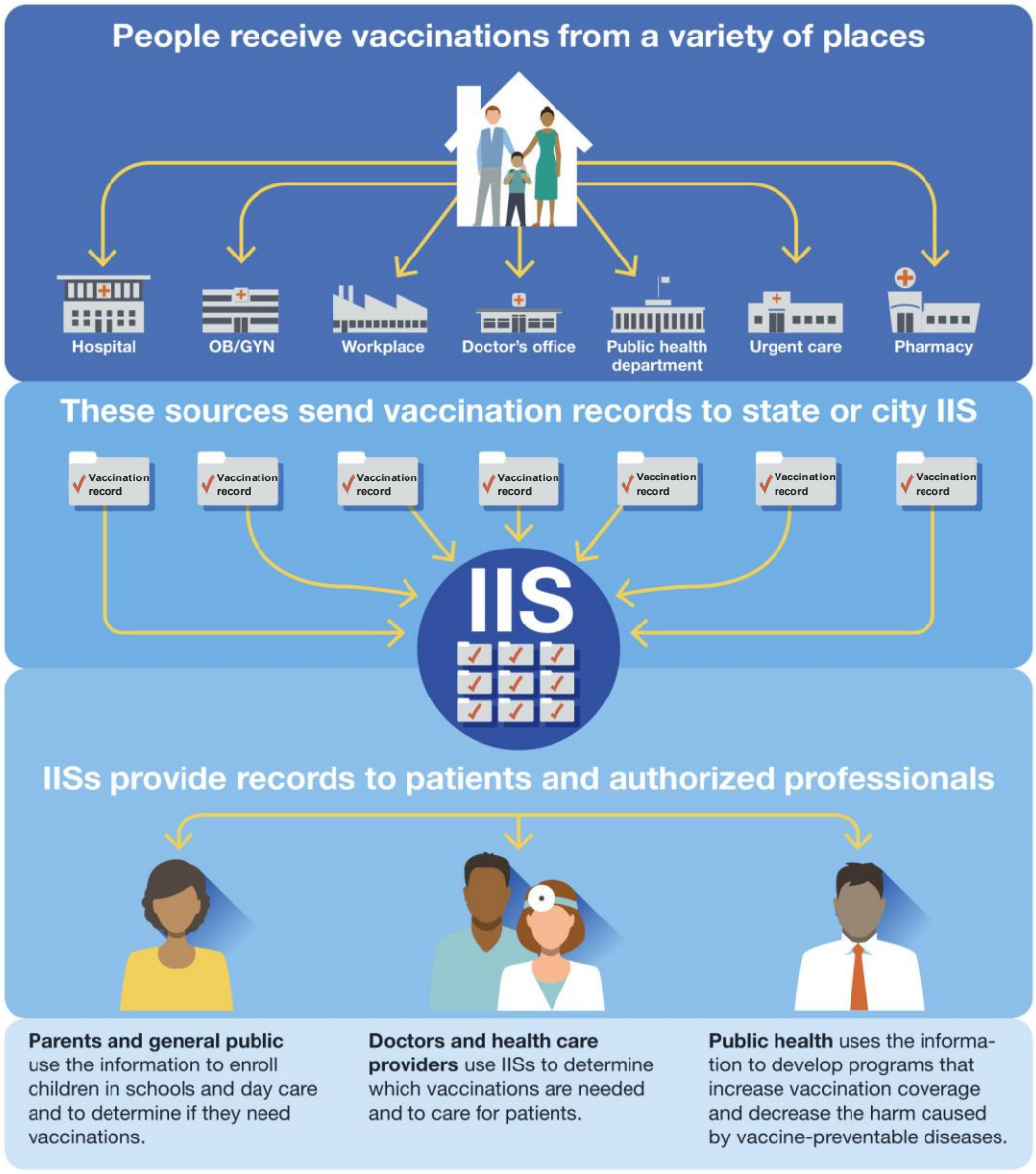
[5] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 (2019)," https://www.cdc.gov/vaccines/programs/iis/functional-standards/func-stds-v4-1.html, accessed January 3, 2023.

[6] *Minnesota Statutes* 2022, 150A.055 and 151.01.

and Monkeypox immunizations, there are no requirements in law that mandate other health care providers to report immunizations into the state's IIS.[7] As a result, MDH encourages, but does not require, health care providers to participate in the state's IIS.[8]

Exhibit 1

Immunization Information Systems



Source: Centers for Disease Control and Prevention, "Basics of Immunization Information Systems (IIS)," https://www.cdc.gov/vaccines/programs/iis/downloads/basics-immun-info-sys-iis-508.pdf, accessed January 20, 2023.

[7] See https://www.cdc.gov/poxvirus/monkeypox/pdf/hhs-monkeypox-vaccination-program-provider-agreement.pdf, accessed October 21, 2022; and https://www.cdc.gov/vaccines/covid-19/vaccination-provider-support.html#requirements, accessed October 21, 2022.

[8] According to the CDC's 2020 Immunization Information Systems Annual Report, approximately 80 percent of all Minnesota providers participated in Minnesota's IIS. This was below the CDC's target of 90 percent participation, which only 9 jurisdictions nationally achieved.

Minnesota Immunization Information Connection

Minnesota's IIS, the Minnesota Immunization Information Connection (MIIC), was created in 2002 by the Minnesota Department of Health (MDH). MIIC is based on an IIS software platform developed by the state of Wisconsin—the Wisconsin Immunization Registry (WIR)—which is currently used by 15 states and the U.S. Virgin Islands.

The web-based system is available to participating health care providers, public health agencies, schools, and child care centers in Minnesota to look up immunization histories and view recommended vaccinations. Medical providers, pharmacies, and others report administered immunization doses into MIIC.[9] Minnesotans can receive a copy of their immunization record from their health care provider; by requesting it directly from the Minnesota Department of Health; or by utilizing a smartphone-based application, Docket, which interfaces with the MIIC system.[10]

MDH and other public health officials also use MIIC data for reporting vaccination rates and to help combat disease outbreaks and reduce vaccine-preventable diseases. With timely reporting of immunization doses from medical providers, MIIC helps MDH officials to:

- Ensure health care providers can determine what immunizations their patient needs.
- Analyze vaccination trends and develop strategies to improve immunization rates.
- Generate immunization reminder and recall notices.
- Report immunization data to the public and the federal government.
- Track state-supplied vaccine inventory, waste, and spoilage.

MIIC contains information on more than 127.5 million immunization doses administered for more than 9.5 million individuals, including both living and deceased persons. These records represent people who have received immunizations in Minnesota, including nonresidents of the state, such as people who have moved out of state, and college students or other seasonal residents who received an immunization while visiting Minnesota. These records also include persons born in Minnesota who may have never received a vaccination.[11]

MIIC by the Numbers

MIIC contains records for more than:

- 9.5 million people.
- 127.5 million immunization doses administered.

MIIC is accessed and used by:

- Almost 6,000 organizations.
- More than 16,000 users.

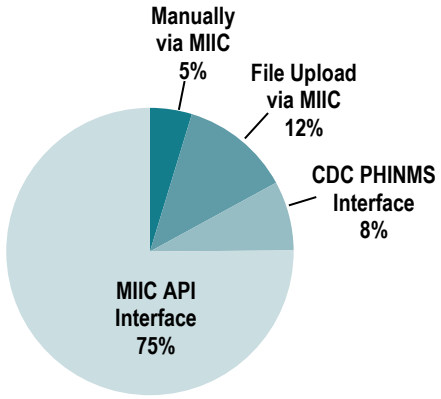
[9] As noted previously, Minnesota laws require pharmacies and dentists to report immunizations in MIIC. Other health care providers voluntarily participate in MIIC.

[10] Minnesota Department of Health, "Find My Immunization Record," https://www.health.state.mn.us /people/immunize/miic/records.html, accessed March 3, 2022, provides instructions for utilizing the Docket mobile phone application and for submitting a record request to the department.

[11] MIIC receives information on births and deaths from the Minnesota Department of Health Office of Vital Records. Data for newborns and individuals receiving immunizations are entered into MIIC unless a parent (on behalf of their child) or individual opts out.

Authorized MIIC users may access MIIC directly by using (a) the system's web-based user interface to enter or retrieve immunization data manually or (b) an interfaced system.[12] Users accessing MIIC via the web-based user interface typically belong to smaller medical, educational, or child care organizations. Medical providers with Electronic Health Record (EHR) systems may automatically interface with MIIC to insert, update, delete, and retrieve immunization data.[13] This electronic interface is more common at mid- to large-sized medical providers. MIIC allows interfacing via the CDC's Public Health Information Network Messaging System (PHINMS) or its own MIIC Application Program Interface (API). Some student information systems at educational facilities also interface electronically with MIIC to retrieve student immunization data. In 2004, nearly 88 percent of all reporting was by direct entry into the web-based application.[14] By 2021, as depicted in Exhibit 2, only 5 percent of all immunization entries were submitted manually, with approximately 83 percent being submitted through an electronic interface.

Exhibit 2
2021 MIIC Immunization Data Entry Method



Source: Office of the Legislative Auditor.

MIIC Funding

MDH relies upon federal funds administered through the CDC to pay for the maintenance, support, and further development of the MIIC system.[15] Accordingly, MDH and MNIT must balance system maintenance, security, and ongoing support with work to complete grant deliverables. Minnesota's approach is not unique. According to the American Immunization Registry Association, less than 50 percent of jurisdictions have local or state funding for their IIS maintenance, operations, and enhancements.[16]

Data Collection and Sharing

There are two key laws—one at the federal level and one at the state level—that govern the privacy of protected health information (PHI). The primary federal regulation is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.[17] The primary state regulation is known as the Minnesota Health Records Act.[18]

---

[12] Authorized MIIC users include health care providers, school personnel, pharmacists, and others identified as able to share immunization data under *Minnesota Statutes* 2022, 144.3351, and who are associated with a participating organization.

[13] Systems interfacing with MIIC use an industry standardized Health Level Seven (HL7) message structure.

[14] Sripriya Rajamani, Erin Roche, Karen Soderberg, Aaron Bieringer, "Technological and Organizational Context around Immunization Reporting and Interoperability in Minnesota," *Online Journal of Public Health Informatics* (December 15, 2014).

[15] Public Health Services Act, codified as 42 *U.S. Code*, sec. 247b(m)(3)(I) (2010).

[16] American Immunization Registry Association, Immunization Information System (IIS) Information Session, April 15, 2021.

[17] 45 *CFR*, pt. 164, subp. E (2018).

[18] *Minnesota Statutes* 2022, 144.291, subd. 1.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created national standards to protect patient health information from being disclosed without the patient's consent or knowledge. Health care providers, health plans, health care clearinghouses, and business associates (those doing business with a covered entity) that transmit certain health care information electronically are considered *covered entities* and must adhere to HIPAA's privacy rule.[19] MDH is not considered a covered entity under HIPAA, rather it is a *public health authority*.

HIPAA permits certain uses and disclosures of protected health information (PHI) without the patient's authorization to public health authorities, including for the purpose of preventing or controlling disease. Since MDH is classified as a public health authority under HIPPA, it and similarly covered entities may exchange information for these purposes without an individual's authorization.[20]

Minnesota Health Records Act and Immunization Data Sharing Law

The Minnesota Health Records Act protects patient health information from being disclosed without the patient's consent or knowledge.[21] However, Minnesota statutes allow immunization data to be shared among MDH, health care providers, group purchasers (including insurance companies), postsecondary educational institutions, elementary and secondary schools, child care facilities, community health boards, and community action agencies without the individual's consent, if the person requesting the data provides services on behalf of the individual.[22] Immunization data includes information such as name; address; date of birth; gender; parent/guardian's name; and vaccination information, such as date of immunization, immunization type, manufacturer, lot numbers, and contraindication or adverse reaction information.[23] MIIC also includes additional information, such as the individual's phone number, e-mail address, mother's maiden name, birth and death information, and racial and demographic information that help to identify the individual and aid in public health activities. MIIC does not contain an individual's social security number or a unique health identifier.

Immunization Data Includes

- Name
- Address
- Date of birth
- Gender
- Parent/guardian's name
- Vaccination information
  - Date of immunization
  - Immunization type
  - Manufacturer
  - Lot numbers
  - Contraindication or adverse reaction information

— *Minnesota Statutes* 2022, 144.3351

[19] 45 *CFR*, pt. 164, subp. E (2018).

[20] 45 *CFR*, sec. 164.512 (2018).

[21] *Minnesota Statutes* 2022, 144.293.

[22] *Minnesota Statutes* 2022, 144.3351.

[23] *Ibid*.

OLA

Audit Scope, Objectives, Methodology, and Criteria

The Office of the Legislative Auditor (OLA) conducted this audit to determine whether the Minnesota Department of Health (MDH) and Minnesota Information Technology Services (MNIT) have adequate internal controls to safeguard the confidentiality, integrity, and availability of the Minnesota Immunization Information Connection (MIIC) system and its data. Secondarily, we assessed compliance with applicable Immunization Information System Functional Standards recommended by the Centers for Disease Control and Prevention (CDC).

We assessed risks within the MIIC environment focusing primarily on the following controls:

- Data management
- Logging and monitoring
- Data integrity
- Access/account management
- Change management
- Disaster recovery
- Risk assessments and mitigation

We designed our work to address the following questions:

- Do MDH and MNIT have appropriate controls in place to secure the MIIC system and protect its private data?
- Is there integrity to the MIIC data, such that it does not contain inaccurate or improbable data?

To answer these questions, OLA auditors:

- Reviewed agency procedural documentation and interviewed MDH and MNIT staff to gain an understanding of applicable controls.
- Tested a sample of the MIIC privacy-setting change requests.
- Analyzed the full population of MIIC client and immunization data to identify potentially duplicate or improbable data.[24]

[24] The Minnesota Department of Health refers to people who have records in MIIC as clients. The term client is interchangeable with patient or individual, depending on the context.

- Reviewed current system configuration documentation, system security assessments, system vulnerability scan results, and risk management practices.
- Examined select user access account information and permissions for both the MIIC system and its underlying database.
- Examined system change documentation and related communications.
- Tested a sample of individual system changes.
- Reviewed MIIC disaster recovery plans for completeness and accuracy.

While OLA gained an understanding of funding sources for MIIC, we did not audit budgets or expenses associated with the system. Other MIIC functions, such as vaccine ordering and fulfillment and public access via the Docket smartphone application, also were outside the scope of our audit.

In addition, OLA gained an understanding of physical security controls. However, based upon our review of the independent audit of MNIT's vendor, which did not identify any significant exceptions with the physical security controls over the MIIC hardware or its related data center, we did not conduct any testing.

We conducted this information technology performance audit in accordance with generally accepted government auditing standards.[25] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Using applicable and relevant federal and state laws, Centers for Disease Control and Prevention functional system standards, and agency policies and standards, we tested whether MDH and MNIT had effective controls in place to protect the confidentiality, integrity, and availability of the MIIC system.

To assist with our testing and validation of data, OLA obtained access to the MIIC system and a database containing MIIC system data.[26] When sampling was used, we used a sampling method that complies with generally accepted government auditing standards and that supports our findings and conclusions. That method does not, however, allow us to project the results we obtained to the populations from which the samples were selected.

[25] Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards* (Washington, DC, July 2018).

[26] Testing of MIIC data was as of April 14, 2022.

Minnesota Immunization Information Connection Audit Testing

Data Use Agreements

Centers for Disease Control and Prevention (CDC) functional standards stipulate that all IISs should have agreements with organizations and individual users of the IIS to address confidentiality and data use. The CDC standards also recommend these user agreements to be regularly updated.[27]

Prior to participating in and accessing the Minnesota Immunization Information Connection (MIIC), the Minnesota Department of Health (MDH) requires organizations and individual users to read and sign a Data Use Agreement (agreement). The agreement defines the responsibilities of organizations and individual users to protect private data. Organizations must renew their agreement every three years, while individual users must renew their agreements annually.

The agreements define allowable uses of MIIC and its information in accordance with state statute.[28] The agreements state that MIIC can be used to:

- Assess an individual's immunization status to determine needed immunizations.
- Issue reminder notices to individuals due or past due for immunizations.
- Notify an individual of a vaccine-preventable disease outbreak that may affect them.
- Produce individual immunization reports for school admission, child care enrollment, or other processes that require an immunization history.
- Notify an individual of vaccine recalls.
- Prepare summary reports without personally identifiable information.
- Facilitate the ordering and management of state-supplied vaccines.

Organizational agreements include additional requirements, such as:

- Designating an administrator for MIIC who is responsible for establishing and overseeing individual user accounts within the organization.
- Prominently displaying and/or distributing information about MIIC that notifies individuals of their option not to participate.
- Ensuring MIIC data privacy and security, including but not limited to:
    - Inactivating users' accounts within one business day of voluntary employment termination or transfer, or in cases of involuntary

[27] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 4.2-4.5." (2019).

[28] *Minnesota Statutes* 2022, 144.3351.

termination, inactivating the account prior to notifying the employee of the termination.

- Ensuring that any system used to access MIIC is up to date on all software patches and updates.
- Auditing user activity, if the organization accesses MIIC via an Electronic Health Record interface.
- Ensuring that any subcontractors used by the organization to help access, aggregate, and/or transport immunization data to or from MIIC also abide by the terms of the user agreement.

Using data analytics, we confirmed that all active individual users of MIIC had current agreements recorded. We also found that MDH had reasonable controls to require regularly updated user agreements. We validated that MIIC has automated controls during its login processes that requires individual users to accept and renew these agreements. When the individual agreements are electronically signed, the system logs the acceptance.

Completion of organizational agreements is a less automated process; MIIC is not programmed to require updates of expired agreements before granting access to the system. Nevertheless, MDH tracks the status of organizational agreements within MIIC. Using data analytics, we examined whether all active organizations had completed a data use agreement within the past three years. Our testing revealed MDH had valid data agreements.

While there is no CDC standard that recommends MDH to audit users' compliance with the terms of the data use agreements, the state's internal control framework sets an expectation that MDH monitor such agreements.[29]

FINDING 1

MDH does not actively monitor whether users or participating organizations with access to MIIC comply with data use requirements.

Although data use agreements contain a provision that allows MIIC representatives to monitor the participating organizations, they generally do not do so.[30] MDH told us they would investigate and act based on a complaint or noticeable abuse, but said they do not have the resources to perform additional monitoring.

Without monitoring and oversight, MDH cannot be confident that organizations and users are following data use requirements and ensuring the privacy and security of MIIC data. For example, MDH lacks certainty that organizations (health care

[29] Minnesota Management and Budget adopted the U.S. Government Accountability Office's established definitions of internal control, standards, internal control components, principals, and attributes; and Comptroller General of the United States, Government Accountability Office, *Standards for Internal Control in the Federal Government* (known as the Green Book), Principle 16 – Perform Monitoring Activities, pp. 65-67 (Washington, DC, September 2014).

[30] MDH data use agreements stipulate that a "MIIC representative" is an MDH staff person or contractual regional representative of MIIC who provides outreach and training on use of MIIC.

providers, schools, child care facilities, and community action agencies) are timely removing access when employees leave the organization.

RECOMMENDATION

MDH should monitor users and organizations to ensure compliance with data use agreements.

Logging and Monitoring

The CDC's functional standards include recommendations for the creation and storage of an audit log, which identifies the date and time a user creates, views, or modifies a record in an IIS system.[31] For systems containing sensitive data, like MIIC, Minnesota Information Technology Services' (MNIT's) information security logging and monitoring standard requires that certain actions be logged to ensure the effective detection, response, and handling of information security events or incidents.[32]

FINDING 2

MIIC does not meet all of the requirements defined within MNIT's logging and monitoring standard.

When an authorized user is granted access to MIIC, the system generally provides a broad level of access within the system. With such broad access, logging and monitoring are important to help to identify inappropriate access to records.

Although MIIC includes some logging functionality, it does not meet all of the requirements defined within MNIT's logging and monitoring standard. Due to the sensitivity of this issue, we are not including all elements of a finding in this report. We communicated the details of this issue separately to MDH and MNIT.

RECOMMENDATIONS

- **MDH and MNIT should implement logging functionality to comply with MNIT's logging and monitoring standard.**
- **MDH and MNIT should implement a process to regularly review and monitor MIIC audit logs, specifically looking for unusual or unauthorized activities.**

[31] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 5.5." (2019).

[32] Minnesota Information Technology Services, *Security Monitoring and Response Policy*, version 1.4, March 10, 2020; and Minnesota Information Technology Services, *Security Logging and Monitoring Standard*, version 1.6, October 1, 2022.

Opting Out of MIIC

Neither federal nor Minnesota law requires individuals to consent to have their immunization records included in MIIC. Similarly, neither federal nor Minnesota law requires MDH to offer individuals the ability to withdraw consent or limit participation in MIIC. By default, individuals who are born in, or receive immunizations in Minnesota, participate in MIIC. However, MDH allows individuals to withdraw their consent, limit access to their MIIC data to an individual health care provider, or opt-out of MIIC entirely.

As part of our audit, we reviewed the process for limiting access or opting out of MIIC, and evaluated whether MDH followed its processes when it received such a request.

The MIIC data use agreements stipulate that participating organizations must display or distribute information that notifies individuals of their option not to participate in the system. The data use agreements further stipulate that no individual will be penalized for choosing not to participate in MIIC.

MDH provides a process by which parents (on behalf of their children) or individuals can complete a form to limit or prevent access to MIIC records.[33] Individuals can select different levels of privacy control over their data, as follows:

- **Decline immunization reminders:** The individual's MIIC record is excluded from queries and reports generated to produce reminders.

- **Limit access to a single provider organization:** MDH locks the individual's MIIC record and allows view access to only the specified health care provider organization.

- **Opt out and seal:** The individual's MIIC record is excluded from queries and reports generated to produce reminders. In addition, MDH locks the MIIC record and prevents any view access. The record will still be updated as the individual receives new immunizations.

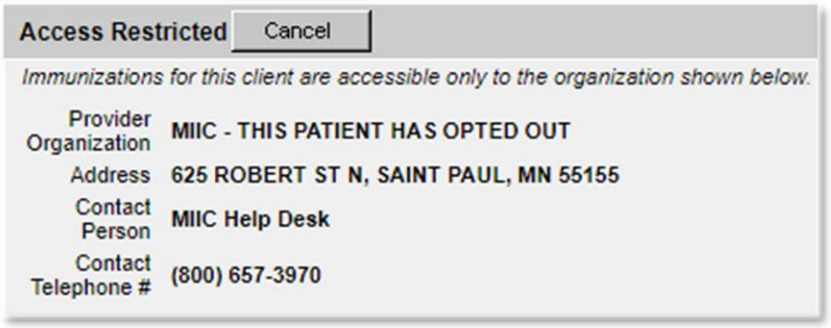
- **Opt out and purge:** The individual's MIIC record is excluded from queries and reports generated to produce reminders. MDH also locks the MIIC record and retains certain identifiable information to prevent re-entry, but removes all immunization history from the MIIC database. An automated process ensures any future updates to the immunization record, such as new immunizations received, are removed daily.

Once an individual submits the form, MDH staff review and process the request. When a MIIC record is restricted to a single medical provider or the individual has opted out, MIIC users attempting to access the record receive a message stating that access to the

[33] Minnesota Department of Health, "Data Privacy and MIIC Records," https://www.health.state.mn.us /people/immunize/miic/privacy/dataprivacy.html, accessed November 1, 2022.

record has been restricted. If access is limited to a single medical provider, the message identifies the provider. Exhibit 3 shows the message displayed in MIIC when an individual opts out.

Exhibit 3
MIIC Access Restricted Message



Source: Minnesota Department of Health, Minnesota Immunization Information Connection (MIIC).

According to MDH data, the agency received approximately 6,700 privacy setting change requests in 2021. To verify that requests were properly processed, OLA tested a sample of 25 of these change requests and found that MDH had properly locked the individual's MIIC records, as well as purged the immunization history records where appropriate. We found no exceptions in our testing.

MIIC Data Integrity and Reliability

Data integrity and reliability is the assurance of the accuracy and consistency of data. It is important for MIIC to have accurate and complete records to be of the most value to users of the system.

OLA tested the integrity and reliability of certain data in MIIC. After gaining an understanding of certain data quality controls, we analyzed MIIC data specifically looking for invalid or improbable data.

Improbable Immunizations

MIIC contains a variety of rules that prevent a user from entering improbable immunization data, such as vaccinations occurring in the future, prior to an individual's date of birth, or after an individual's date of death. These rules help to ensure that the data within MIIC are accurate. Exhibit 4 displays MIIC's user interface notifications that the user receives when entering certain invalid immunization data. As an additional control, MDH regularly runs an "Improbable Shots" report, which MDH staff use to identify, and follow up on, obsolete vaccine codes or immunizations given outside of typical age-ranges.

Exhibit 4

MIIC Exception Notifications

Source: Minnesota Department of Health, Minnesota Immunization Information Connection (MIIC).

We queried all vaccinations in the MIIC database to determine if MIIC contained any entries that violated these rules. Our testing identified no significant deviations related to immunizations dated as having been given in the future, before birth, or after death.[34]

Duplicate Clients or Immunization Records

CDC functional standards state that all IISs should identify, prevent, and resolve duplicate patient records and immunization events using automated processes.[35] Although MIIC is not an official medical record system for an individual, if information is duplicated in the system, the individual's health care provider may not have a full or accurate view of that individual's immunization history. Further, widespread duplication of individuals and/or immunization records could affect the accuracy of aggregate reporting.[36]

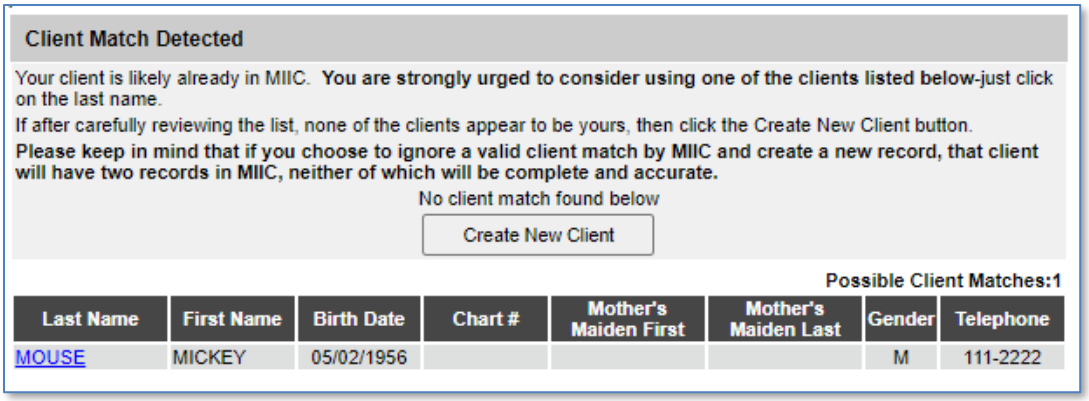
[34] OLA noted minor deviations in historical MIIC data which showed approximately 300 immunizations given prior to individuals' birthdates. We also noted minor deviations in MIIC data showing immunizations given after individuals were deceased. We discussed these minor data deviations with MDH to better understand the controls for each scenario, such as the dates the controls were implemented and any potential bypass of system controls. The agency's response and our follow-up analysis allowed us to conclude this was not a significant concern.

[35] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 2.0-3.0." (2019).

[36] MIIC is inherently at risk of containing duplicate client records, as MDH does not collect social security numbers or use a unique identification number to identify an individual's record. Instead, the system uses demographic information, such as name and date of birth, to identify an individual's record.

MIIC utilizes two automated processes to detect and flag potential duplicate records when they are entered into the system. First, when an individual user manually enters data into MIIC, the system will notify the user when it identifies a potential duplicate record. The user then has the option to use the existing identified client record or to create a new record. Exhibit 5 shows the MIIC prompt displayed to the user for a potential duplicate record.

Exhibit 5
MIIC Client Match Detected Prompt


Client Match Detected

Your client is likely already in MIIC. **You are strongly urged to consider using one of the clients listed below-just click on the last name.**

If after carefully reviewing the list, none of the clients appear to be yours, then click the Create New Client button.

Please keep in mind that if you choose to ignore a valid client match by MIIC and create a new record, that client will have two records in MIIC, neither of which will be complete and accurate.

No client match found below

Create New Client

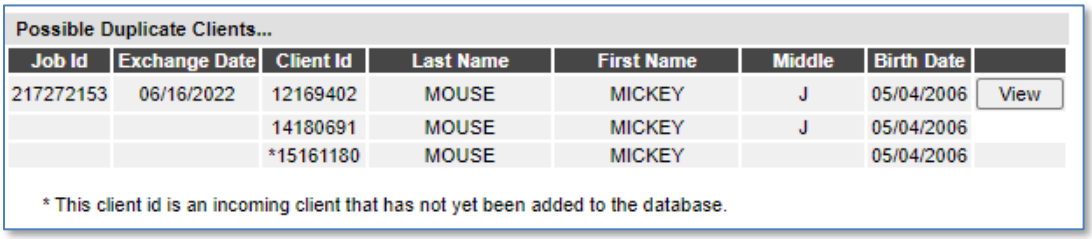
Possible Client Matches:1

Last Name	First Name	Birth Date	Chart #	Mother's Maiden First	Mother's Maiden Last	Gender	Telephone
MOUSE	MICKEY	05/02/1956				M	111-2222

Source: Minnesota Department of Health, Minnesota Immunization Information Connection (MIIC).

Second, when health care providers enter a patient into their Electronic Health Record (EHR) system, and the data interfaces with MIIC, system edits place possible duplicate records into a *pending* status. MIIC staff review this pending information to determine whether the client is indeed a duplicate. If it is a duplicate, staff are able to merge the records. Exhibit 6 shows the prompt for possible duplicate patients, including a pending client record that has not yet been added to the MIIC database.

Exhibit 6
MIIC Possible Duplicate Clients


Possible Duplicate Clients...

Job Id	Exchange Date	Client Id	Last Name	First Name	Middle	Birth Date	
217272153	06/16/2022	12169402	MOUSE	MICKEY	J	05/04/2006	View
		14180691	MOUSE	MICKEY	J	05/04/2006	
		*15161180	MOUSE	MICKEY		05/04/2006	

* This client id is an incoming client that has not yet been added to the database.

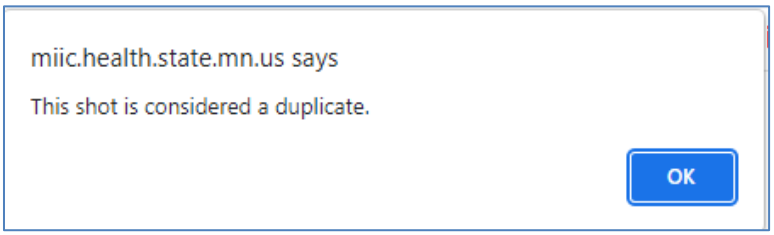
Source: Minnesota Department of Health, Minnesota Immunization Information Connection (MIIC).

MIIC contains similar functionality to prevent duplicate immunizations. Immunizations entered via the application interface are considered duplicate and flagged as "Not Valid" when they are from the same vaccine group and administered within three days of an already existing immunization record. MDH staff can review these potential duplicate immunizations and delete any invalid entries.

If a health care provider manually enters a duplicate immunization into MIIC, the user receives a notification at the time of entry, and the system rejects and does not save the duplicate record. Exhibit 7 shows the exception message that the user receives.

Exhibit 7

MIIC Duplicate Immunization Exception Message



Source: Minnesota Department of Health, Minnesota Immunization Information Connection (MIIC).

We analyzed the data contained within MIIC to determine the extent to which the database contains duplicate records. We queried the MIIC database to identify individuals with identical first names, last names, and dates of birth. We identified one half of one percent (0.5 percent) of the total number of individuals within MIIC as having potentially duplicate client records. Given the limitations of the data, we believe that the actual number of duplicate records is lower.

We also analyzed MIIC data to identify potential duplicate immunization events recorded for the same person. We queried the MIIC database to identify any individuals where MIIC records indicated that they received more than one immunization of the same vaccine on a single day. Because our testing identified no significant deviations, we believe with reasonable assurance that the controls within MIIC are generally effective to identify, prevent, and resolve duplicated client records and immunization events.

Test and Training Data in MIIC

MNIT's Secure Systems Development and Acquisition Standard states that production systems should not be used for testing.[37] Data entered for testing and training purposes could skew reports generated from a production system, such as the reports of statewide vaccination rates that MDH generates from MIIC data.

FINDING 3

MIIC contains testing and training data in the production system.

As part of our analysis, we examined MIIC records to determine whether they contained testing or training data that were unlikely to be tied to real people or actual immunization events. Our testing queried the MIIC database for obvious unlikely names, including:

- First or last names containing "ZZZ," "TEST," or "TRAINING."
- Names containing fictional characters, such as "MICKEY MOUSE" or "SPONGE BOB."

[37] Minnesota Information Technology Services, *Secure Systems Development and Acquisition Standard*, version 1.5, November 1, 2021.

Based on these parameters, we identified 572 probable test or training client records, linked to 2,735 immunizations. When asked, MIIC staff confirmed that MDH uses the production MIIC system for certain testing and training. Staff told us that this testing is done under a specific organization unit number and provided evidence showing that this organization unit is excluded from any immunization reporting. However, 392 of the test or training client records, linked to 2,317 immunizations, were entered without the specific test unit number. Further, we traced these records to various external health care providers and organizations. Entering test data into MIIC could be considered a breach of the organizations data use agreement.[38] MIIC staff told us that they discuss test data with medical providers during the onboarding process to MIIC and inform providers that they should not enter test data into the MIIC production system.

In the overall context of MIIC's more than 9.5 million client records containing information on 127.5 million immunization doses administered, the identified test and training data account for no more than 0.004 percent of all client records and 0.002 percent of all immunization records tracked in the system. However, not all test scenarios were part of our audit testing, which leaves the risk that other test and training data exist in the production system. As a result, these data could impact the accuracy of aggregate MIIC reporting.

RECOMMENDATIONS

- **MDH and MNIT should educate MIIC users not to enter test and training data into the production system.**
- **MDH and MNIT should have adequate controls to identify or prevent test and training data from entering into the production system.**

Account and Access Management

The CDC's IIS standards include recommendations for managing system accounts in accordance with industry security standards.[39] Similarly, MNIT has identity and access management standards that align with the National Institute of Standards and Technology (NIST) industry guidance.[40] We evaluated the extent to which MIIC application controls aligned with the CDC functional standards and MNIT's identity and access management standards. In particular, we performed testing to validate that:

- Unique credentials were utilized for each user or system interface of MIIC.

[38] The Minnesota Department of Health data use agreements stipulate that organizations should ensure that users do not enter inaccurate data, or falsify data currently in MIIC, neither knowingly nor negligently.

[39] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 5.0-5.6." (2019).

[40] Minnesota Information Technology Services, *Identity, Credential, and Access Management Policy*, version 1.4, March 10, 2020; Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.4, March 10, 2020; and U.S. National Institute of Standards and Technology, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 2020, section 3.1, pp. 18-58, describes industry standards for identity and access management that organizations should implement for information systems.

- Password controls were properly implemented.
- Application database access was adequately limited.
- Security roles limited system access based on job responsibilities.
- Accounts and privileges no longer required were timely removed or disabled.

Our testing of security roles and timely removal of access was limited to state employees. We did not test the effectiveness of access management controls for users outside of MDH and MNIT.

In general, we found account management controls to be operational and in compliance with MNIT and CDC standards. Our testing found no significant findings.

System Change Management

Best practices dictate that MDH and MNIT should have business processes to ensure changes made to information systems, such as MIIC, go through a systematic review and approval.[41] These changes can occur to system configurations, computer code, or data. Changes that do not follow a systematic approach have a greater risk of causing adverse issues with system availability, system integrity, and/or data confidentiality.

MDH and MNIT teams utilize an Agile development methodology to manage ongoing maintenance and enhancements to the MIIC system.[42] The Agile process helps to keep all team members (including business and technical staff) aware of the work being performed and upcoming system changes. The team's process also includes MNIT Enterprise Change Management procedures.[43] We tested a sample of system changes to validate that MDH and MNIT followed a systematic change management approach.[44] Our sample included checks of:

- Business testing and acceptance.
- Security vulnerabilities.
- Notices and approvals processed through a change management board.
- Controlled production releases.

In general, we found no significant change management issues.

---

[41] As a basis to define industry best practices, we used the U.S. National Institute of Standards and Technology, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 2020; and ISACA's COBIT 2019, a framework for the governance and management of information and technology.

[42] Agile development is a term used to describe iterative software development that is typically completed in short increments.

[43] Minnesota Information Technology Services, *Change Management Process Definition Document*, version 3.04, March 22, 2022.

[44] We randomly sampled 15 system changes related to five MIIC software releases between July 1, 2021, and February 28, 2022.

In addition to evaluating the change management processes used for MIIC and comparing them to best practices and MNIT defined procedures, we also assessed compliance with applicable information security requirements within MNIT's Secure Systems Development and Acquisition Standard.[45]

MNIT's security standard requires that, prior to releasing new or updated applications to production, all code must be reviewed, and the review must include use of specialized coding analysis software. Source code security analysis tools scan a textual (human readable) version of source files that comprise a portion or all of an application program. These files may contain inadvertent or deliberate weaknesses that could lead to security vulnerabilities in the executable versions of the application program. Source code security analysis tools assist development teams with finding and fixing vulnerable code. Use of a source code security analysis tool does not guarantee the code will be free of weaknesses. However, when combined with other secure software development controls, it provides additional assurance of detecting some of the most prevalent and highly exploitable security weaknesses.

FINDING 4

MNIT did not use code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software.

As a general practice, the MNIT team working on MIIC only scan MIIC software with code analysis software when significant changes are made. Although it may not be practical to scan all code for security vulnerabilities with each Agile application update, the MNIT development team did not have an approved exception to the policy.[46] Furthermore, the development team did not have clear criteria defining "significant changes" for when these scans should occur.

While there are greater risks with significant software updates, even small coding changes can introduce security vulnerabilities. Uncorrected, these vulnerabilities could be discovered and exploited, potentially resulting in a privacy breach or corrupt data. Finding the correct balance between security and Agile development requires active risk management discussions and approval from the right level of management.

RECOMMENDATION

MNIT should utilize code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software.

[45] Minnesota Information Technology Services, *Secure Systems Development and Acquisition Standard*, version 1.5, November 1, 2021.

[46] MNIT's policies and standards define the minimum set of controls necessary to ensure data and systems are adequately secured. In accordance with MNIT's risk treatment procedures, if a control is not in place, that control, along with a remediation plan to address the gap or an approved exception, must be documented, tracked, and managed. Appendix A outlines MNIT's Risk Treatment Procedure.

Our testing identified three system security vulnerabilities within MIIC that were not identified as part of MNIT's code review.

FINDING 5

MIIC contained exploitable vulnerabilities that could have allowed a compromise of user accounts and private data.

Due to the severity of these issues, we are not including a description of the vulnerabilities in this report. We communicated the details of these issues to MDH and MNIT during our audit to allow them to take corrective action prior to the release of this report. MNIT staff responsible for maintaining MIIC told us they were previously unaware of these specific vulnerabilities.

These vulnerabilities could have enabled an attacker to exploit flaws in the MIIC system to obtain access to user accounts and private data.

RECOMMENDATIONS

- **MDH and MNIT should prioritize mitigation of known MIIC system vulnerabilities.**
- **MDH and MNIT should regularly perform manual information security testing to ensure that system changes do not introduce vulnerabilities into the MIIC system.**

Disaster Recovery

Disaster recovery planning for information technology systems ensures that state agencies are prepared to restore or recover priority systems if and when service interruptions occur.[47] Recognizing the importance of IISs, the CDC includes disaster recovery recommendations within its functional standards.[48] At the local level, Minnesota Executive Order 19-23 requires each state entity to develop a Continuity of Operations Plan and outlines what should be included in the plan. The order requires MNIT to establish information technology disaster recovery (ITDR) plans that align with agencies' priority services.[49]

MNIT has established an Information Technology Disaster Recovery Planning Policy and an Information Technology Disaster Recovery Planning Standard outlining disaster

[47] The Office of the Legislative Auditor released a related audit in September 2022, to determine whether MNIT and selected state agencies had disaster recovery plans to minimize the recovery time of key systems if a major disruptive event or disaster were to occur. MIIC was not one of the four systems included in the scope of that audit. Office of the Legislative Auditor, Financial Audit Division, *Disaster Recovery Strategies for Critical IT Systems* (St. Paul, September 2022).

[48] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 6.4-6.6, and 6.8." (2019).

[49] State of Minnesota Executive Order 19-23, "Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans," April 4, 2019.

recovery planning actions and requirements.[50] The Disaster Recovery Planning Standard requires that disaster recovery plans be developed and maintained for critical systems. The standard also outlines the requirements for information technology disaster recovery planning activities, including plan development, distribution, review, training, and testing; data backup; and alternative site recovery.

MDH has classified MIIC as a "Priority 1" system due to its role in facilitating a statewide response against imminent health threats from vaccine-preventable diseases. The Priority 1 classification means that in the case of a disaster, MIIC must remain uninterrupted or be recovered within 24 hours. The MIIC disaster recovery plan states that the system should be restored immediately, with no downtime.

FINDING 6

In the case of a disaster, MNIT may not meet expected system restoration timelines for MIIC due to an incomplete disaster recovery plan and architecture limitations.

MDH and MNIT have developed a disaster recovery plan for MIIC. However, the plan does not adequately describe and document the strategy to recover MIIC from backup. Further, the system's disaster recovery strategy itself does not support immediate restoration.

In our review of the MIIC disaster recovery plan, we noted that the plan lacked certain details necessary for the recovery of the system. In 2020, MDH and MNIT moved MIIC into a cloud-provider's data center. For operational purposes, and to restore from a disastrous event, MNIT technical staff must have the necessary access permissions to manage MDH's portion of this cloud environment. Staff must also establish a secure connection to this network. However, MNIT staff overlooked these details when making annual updates to the MIIC disaster recovery plan and did not reference these connectivity requirements or the cloud-based environment.

The MIIC information technology disaster recovery (ITDR) plan refers to the system's "implementation plan"—reusing the documented procedures that MNIT uses to build and deploy code to the MIIC servers as part of its normal operational software release processes. While this implementation plan contains valuable steps, in a disaster scenario, the team would need to restore the system from backup, rather than deploy code. While MNIT staff told us that the implementation plan would provide the most current description of the system configuration, they conceded that they had not included restoration procedures. The ITDR plan contains no discussion of the system's backup frequency, the system's current or recovery locations, or procedures necessary to restore the system's database or servers from backup. While the cloud hosting vendor provides many tools for detecting and recovering from system failures, the plan does not mention if, or how, these tools would be used.

[50] Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Policy*, version 1.4, March 10, 2020; and Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Standard*, version 1.4, March 10, 2020.

We further noted that MIIC's current hosting architecture and configuration do not support high system availability or enable automatic failover between data centers. Instead, MNIT staff must manually restore systems. As a result, MNIT cannot achieve an "immediate" recovery—with zero downtime—using the current system architecture. A manual restoration process—even if properly documented—would encounter some downtime. Although the cloud hosting vendor offers solutions for zero downtime, MIIC is not set up for using one of those solutions. The current architecture configuration should allow for system restoration within 24 hours; however, MNIT has not conducted a full system restoration recovery exercise of MIIC to best estimate actual recovery times.

RECOMMENDATIONS

- **MNIT should prepare a full restoration plan describing the necessary procedures to restore MIIC from backup.**
- **Working with MDH, MNIT should develop, implement, and test a strategy to meet the desired recovery time objective for MIIC.**

Risk Assessment and Ongoing Risk Management

The CDC's IIS functional standards include language on conducting regular risk assessments.[51] Such assessments are also a required practice under Minnesota Management and Budget's (MMB's) Risk Assessment Procedure and MNIT's Information Security Standard.[52] MMB's procedures require that agencies annually conduct a high-level, but comprehensive, review of the organization's most significant business processes and risks. MNIT's Information Security Risk Management Standard states, "an information security risk assessment must be performed on all new and significantly changed systems…." For systems like MIIC, with a data protection categorization of high, the MNIT standard requires the risk assessment to be updated at least once every three years.[53]

Risk Assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

— National Institute of Standards and Technology (NIST)

MNIT's requirements for risk management include identifying the likelihood and impact of the risks; documenting risk assessment results in a risk assessment report; and

[51] Centers for Disease Control and Prevention, "Immunization Information System (IIS) Functional Standards, v4.1 – Essential Infrastructure Functional Standards, 6.11." (2019).

[52] Minnesota Management and Budget, Statewide Operating Procedure 0102-01.2, *Risk Assessment*, February 11, 2021; and Minnesota Information Technology Services, *Information Security Risk Management Standard*, version 1.4, March 10, 2020.

[53] MNIT's Data Protection Categorization Standard classifies data as "high" if they are highly sensitive and/or protected by law or regulation. This includes protected health information (PHI).

developing remediation plans for identified information security risks, findings, weaknesses, and deficiencies. MNIT's standards also require that all findings and remediation plans must be documented in a centralized findings management tool to help ensure that the remediation plans are accurate, up to date, and readily available. MNIT's process for managing these risks are articulated in Appendix A.

FINDING 7

MDH and MNIT did not complete a risk assessment on MIIC or use MNIT's central management tool, as required by MNIT's standards.

MDH regularly conducts a high-level, agency-wide risk assessment per the MMB procedure.[54] However, MDH and MNIT have not performed a formal risk assessment for the MIIC system in accordance with MNIT's standards and procedures.[55]

Our discussions with MNIT showed that they utilize several tools to actively manage and monitor the various risks affecting MIIC. For example, MNIT regularly scans MIIC servers for vulnerabilities and analyzes scanning results. MNIT also utilizes risk treatment tools within its cloud-based infrastructure to maintain security of its servers. We also observed that MNIT works with MIIC leadership, as various risks are identified, to prioritize and plan mitigation steps as part of the software development process. However, those actions taken by MDH and MNIT lacked required elements outlined within CDC and MNIT standards.

We found that a formal risk assessment report, containing MNIT's standardized risk rating criteria, was not completed. We also observed a variety of security risks, assessment findings, and policy exceptions that were not logged in the MNIT central risk management tool. Some known, but nonreported, security risks or gaps in controls, and policy exceptions included lack of:

- Multi-factor authentication implementation for access to MIIC.
- Logging capabilities sufficient to comply with MNIT's standards.
- Consistent vulnerability scanning of software updates for MIIC.
- Remediation plans for known vulnerabilities to MIIC.

A thorough assessment of potential risks and vulnerabilities of the system, coupled with a detailed risk management and remediation plan, helps to ensure that the confidentiality, integrity, and availability of sensitive data (such as protected health information) within systems are adequately protected. With MIIC team members not following the required risk management process, it is difficult to know what risks are being mitigated, remediated, or simply accepted by agency leaders.

---

[54] Minnesota Management and Budget, Statewide Operating Procedure 0102-01.2, *Risk Assessment*, February 11, 2021.

[55] Minnesota Information Technology Services, *Information Security Risk Treatment Procedures*, version 1.0, January 1, 2017.

Having a central repository of risks provides a holistic view of the risks across agencies and allows MNIT to better strategize and prioritize remediation efforts. Furthermore, MNIT's centralized procedures provide a uniform process for MNIT to communicate risks to executive branch leaders, ensuring that they are aware of the risks, are involved in remediation efforts, and accept the risks.

RECOMMENDATIONS

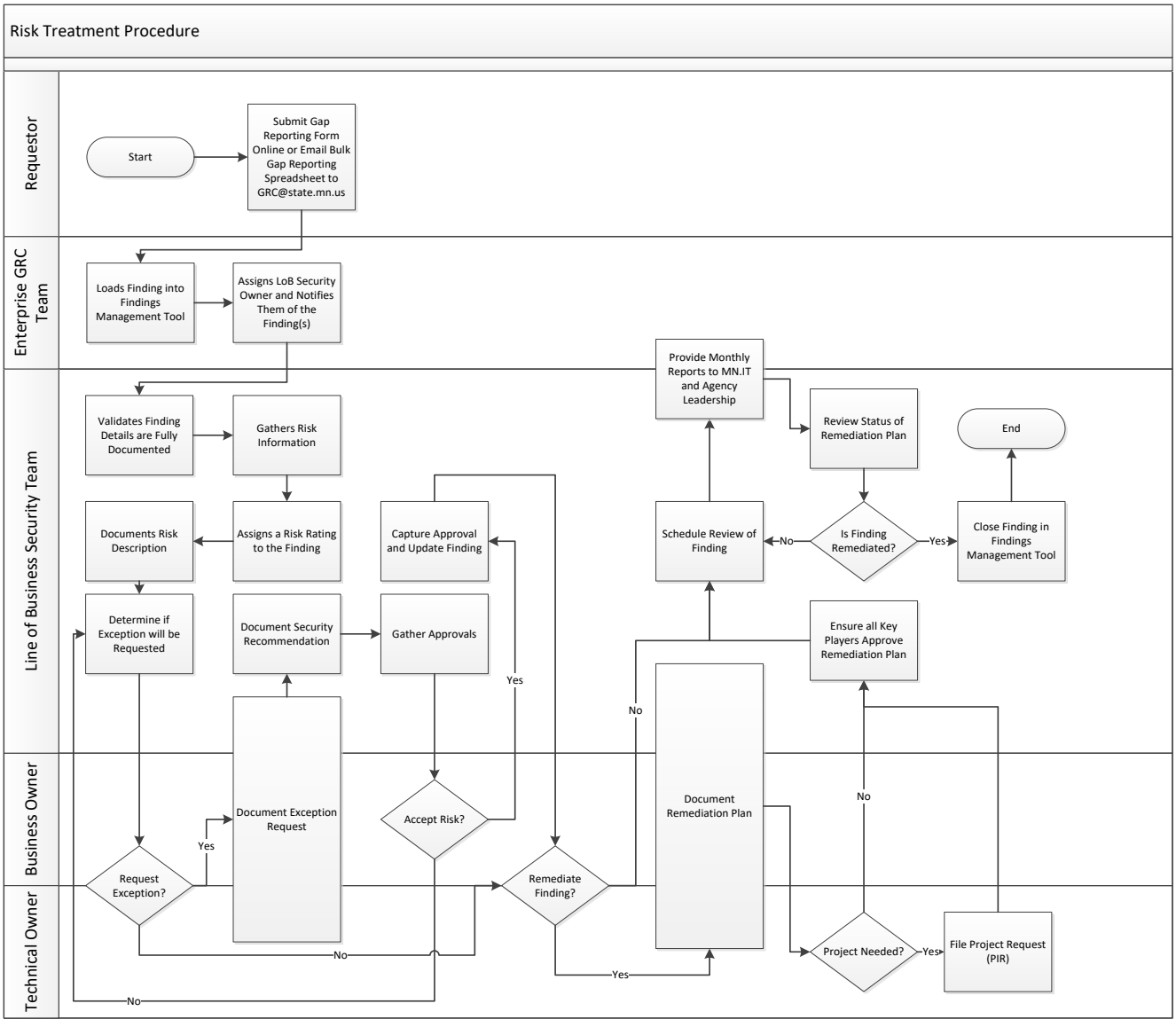
- **MDH and MNIT should perform a risk assessment for the MIIC system according to MNIT standards and procedures.**
- **MDH and MNIT should document known risks, mitigations, and remediations according to MNIT standards and procedures.**
- **MDH and MNIT should utilize the risk assessment to assist with prioritizing risk mitigation efforts and implementing audit recommendations.**

List of Recommendations

- The Minnesota Department of Health (MDH) should monitor users and organizations to ensure compliance with data use agreements. (p. 15)
- MDH and Minnesota Information Technology Services (MNIT) should implement logging functionality to comply with MNIT's logging and monitoring standard. (p. 15)
- MDH and MNIT should implement a process to regularly review and monitor the Minnesota Immunization Information Connection (MIIC) audit logs, specifically looking for unusual or unauthorized activities. (p. 15)
- MDH and MNIT should educate MIIC users not to enter test and training data into the production system. (p. 21)
- MDH and MNIT should have adequate controls to identify or prevent test and training data from entering into the production system. (p. 21)
- MNIT should utilize code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software. (p. 23)
- MDH and MNIT should prioritize mitigation of known MIIC system vulnerabilities. (p. 24)
- MDH and MNIT should regularly perform manual information security testing to ensure that system changes do not introduce vulnerabilities into the MIIC system. (p. 24)
- MNIT should prepare a full restoration plan describing the necessary procedures to restore MIIC from backup. (p. 26)
- Working with MDH, MNIT should develop, implement, and test a strategy to meet the desired recovery time objective for MIIC. (p. 26)
- MDH and MNIT should perform a risk assessment for the MIIC system according to MNIT standards and procedures. (p. 28)
- MDH and MNIT should document known risks, mitigations, and remediations according to MNIT standards and procedures. (p. 28)
- MDH and MNIT should utilize the risk assessment to assist with prioritizing risk mitigation efforts and implementing audit recommendations. (p. 28)

OLA

Appendix A: MNIT's Information Security Risk Treatment Procedure



Source: Minnesota Information Technology Services, *Information Security Risk Treatment Procedure*, version 1.0, January 1, 2017.

OLA

MINNESOTA

January 19, 2023

Ms. Judy Randall
Legislative Auditor
Office of the Legislative Auditor
658 Cedar St. Room 140
Centennial Office Building
St. Paul, MN 55155-1603

Dear Ms. Randall,

Thank you for the opportunity to respond to the findings and recommendations of the Office of the Legislative Auditor's Minnesota Immunization Information Connection (MIIC) Information Technology Audit. The Minnesota Department of Health (MDH) and Minnesota IT Services (MNIT) are responding jointly to this report as our agencies have shared responsibility for this work.

We are pleased to hear that MDH and MNIT generally complied with applicable policies, standards, and best practices. As described in additional detail below, we have already taken significant steps to fully mitigate some of the concerns identified by your auditors and have put steps in place to address the others.

While MDH and MNIT are in the process of replacing our current system, our two agencies have partnered effectively to monitor, maintain, and improve functionality of MIIC within the constraints of existing technology. We have prioritized internal controls to protect the integrity of the data in the system. We are pleased that your office concurs that these controls have been effective to ensure individuals can opt out of the system, that records do not include any improbable immunizations or duplicates, that account and access management complies with MNIT and Centers for Disease Control and Prevention (CDC) standards, and that there were no significant issues or findings in these areas.

Below are our responses to the findings and recommendations in your audit report.

FINDING 1
MDH does not actively monitor whether users or participating organizations with access to MIIC comply with data use requirements.

Recommendation:

- MDH should monitor users and organizations to ensure compliance with data use agreements.

Response:

MIIC users and organizations are required to sign a data use agreement (DUA) that includes requirements to ensure the security and appropriate use of the data in MIIC. MDH frequently monitors our internal controls to assess risk. The requirements in the DUA already provide preventative controls. In addition, MDH will further improve our monitoring by developing an assessment to verify compliance with the DUA requirements. We will require documentation of compliance with applicable terms of the agreement each time an organization renews its DUA.

FINDING 2

MIIC does not meet all the requirements defined within MNIT's logging and monitoring Standard.

Recommendations:

- MDH and MNIT should implement logging functionality to comply with MNIT's Logging and Monitoring Standard.
- MDH and MNIT should implement a process to regularly review and monitor MIIC audit logs, specifically looking for unusual or unauthorized activities.

Response:

There are multiple ways to access MIIC data. The above recommendations apply to less than 1% of queries processed by MIIC on an annual basis. The MIIC system already provides basic logging functionality. We recognize the advantage of meeting all the MNIT logging and monitoring standards. MDH is adopting a new modern system that will implement best practices and fully address the above recommendations. In the meantime, MDH, in partnership with MNIT, is implementing technical changes to improve the functionality of the current MIIC system in this area.

FINDING 3

MIIC data contains testing and training data in the production system.

Recommendations:

- MDH and MNIT should educate MIIC users not to enter test and training data into the production system.
- MDH and MNIT should have adequate controls to identify or prevent test and training client data from entering into the production system.

Response:

Test data is used to simulate real world scenarios without impacting an individual's immunization record. As you note in your report, test data accounts for only 0.004% of all client records and only 0.002% of all immunization records in MIIC. Your report also notes that

a portion of these records are excluded from aggregate MIIC reporting calculations. Our conclusion is that testing and training data in the production system does not impact aggregate MIIC reporting, immunization rate calculations, or public health decision making.

MDH currently provides education to organizations, specifically on the issues of testing and training data. In addition, users and organizations also agree to "not enter inaccurate data, or falsify data currently in MIIC, neither knowingly nor negligently" when they agree to the terms of the annual user agreement and the data use agreement. However, we will provide reminders.

We also have controls in place to prevent substantial test or training data from getting into MIIC. More aggressive controls could cause a negative impact to production data. However, we will continue to monitor our controls and adjust as needed. This finding is resolved.

FINDING 4

MNIT did not use code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software.

Recommendation:

- MNIT should utilize code analysis software to test for security coding vulnerabilities for all of its updates to the MIIC software.

Response:

MNIT completes scans on all major updates. As stated in your report, MNIT completed security scans regularly on MIIC; thirteen scans were conducted between January 2021 and September 2022.

We agree that completing scans on all updates is the best practice and should be done through an automated process (versus the current manual process). MNIT is working to move the MIIC system closer to automated scanning.

FINDING 5

MIIC contained exploitable vulnerabilities that could have allowed a compromise of user accounts and private data.

Recommendations:

- MDH and MNIT should prioritize mitigation of known MIIC system vulnerabilities.
- MDH and MNIT should regularly perform manual information security testing to ensure that system changes do not introduce vulnerabilities into the MIIC system.

Response:

MDH and MNIT have remediated or put controls in place for all identified vulnerabilities. Automated scanning, as referenced in finding 4, will ensure vulnerabilities are not introduced into the system. This finding is resolved.

FINDING 6

In the case of a disaster, MNIT may not meet expected system restoration timelines for MIIC due to an incomplete disaster recovery plan and architecture limitations.

Recommendations:

- MNIT should prepare a full restoration plan, which describes the necessary procedures to restore MIIC from backup.
- Working with MDH, MNIT should develop, implement, and test a strategy to meet the desired recovery time objective for MIIC.

Response:

MNIT has already updated its disaster recovery plan and timelines to accurately reflect a short window of downtime, which meets business needs and still fits in the appropriate timeframe for a Priority 1 service. MNIT has also already updated the plan with the new platforms and restoration procedures to restore MIIC from backup. MNIT has tested the newly updated disaster recovery plan, and it worked as intended. This finding is resolved.

FINDING 7

MDH and MNIT did not complete a risk assessment on MIIC or use MNIT's central management tool, as required by MNIT's standards.

Recommendations:

- MNIT and MDH should perform a risk assessment for the MIIC system according to MNIT standards and procedures.
- MNIT and MDH should document known risks, mitigations, and remediations according to MNIT standards and procedures.
- MDH and MNIT should utilize the risk assessment to assist with prioritizing risk mitigation efforts and implementing audit recommendations.

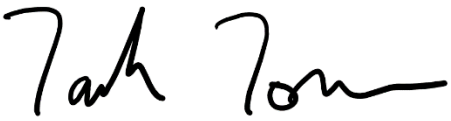
Response:

MDH and MNIT currently complete a risk assessment of MIIC by using Agile development methodologies. Application developers, business owners and security representatives use this methodology to assess risk and application priorities daily. We are working to ensure that the Agile process meets MNIT Standards. In addition, MNIT has reviewed the risk assessment process for MIIC and added a new security risk ranking field into the MIIC work documentation

application. This will assist MNIT and MDH in identifying and managing risk priorities going forward. This finding is resolved.

We appreciate the opportunity to respond to your recommendations and the opportunity to work with you and your team throughout this audit. We appreciate and value the respectful and professional review conducted by your staff. If you have any questions or need additional information, please contact either or both of us.

Sincerely,



Brooke Cunningham, MD, PhD
Commissioner
Minnesota Department of Health
P.O. Box 64975
St. Paul, MN 55164-0975

Tarek Tomes
Commissioner and Chief Information Officer
Minnesota IT Services
658 Cedar Street
Saint Paul, MN 55155

OLA

OLA

OLA

Financial Audit Staff

Judy Randall, *Legislative Auditor*
Lori Leysen, *Deputy Legislative Auditor*

Audit Directors
Ryan Baker
Jordan Bjonfald
Kayla Borneman
Mark Mathison
Heather Rodriguez
Valentina Stone
Scott Tjomsland
Zach Yzermans

Audit Coordinators
Joe Sass

Team Leads
Shannon Hatch
Gabrielle Johnson

Senior Auditors
Tyler Billig
Daniel Hade
Lisa Makinen
Alec Mickelson
Crystal Nibbe
Duy (Eric) Nguyen
Erick Olsen
Sarah Olsen
Amanda Sayler
Emily Wiant

Staff Auditors
Ria Bawek
Nicholai Broekemeier
Andrea Hess
Allison Howk
Zachary Kempen
Sheena Kurth
Zakeeyah Taddese
Peng Xiong

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

To offer comments about our work or suggest an audit, evaluation, or special review, call 651-296-4708 or e-mail legislative.auditor@state.mn.us.

To obtain printed copies of our reports or to obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 711 or 1-800-627-3529.

Printed on Recycled Paper

OLA | OFFICE OF THE LEGISLATIVE AUDITOR

Office of the Legislative Auditor
Suite 140
658 Cedar Street
Saint Paul, MN 55155